NPS ARCHIVE
1997.09
KLEINHANS, C.

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

A PRACTICAL GUIDE TO INTRANET PLANNING

by

Charles D. Kleinhans

September 1997

Thesis Advisor: G. M. Lundy

Approved for public release; distribution is unlimited.

Thesis
K578

DUDLEY KNOX LIBRARY
NAVAL POSTGRADUATE SCHOOL
MONTEREY CA 93943-5101

DUDLEY KNOX LIBRARY
NAVAL POSTGRADUATE SCHOOL
MONTEREY CA 93943-5101

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	September 1997	Master's Thesis

4. TITLE AND SUBTITLE
A PRACTICAL GUIDE TO INTRANET PLANNING

5. FUNDING NUMBERS

6. AUTHOR(S)
Kleinhans, Charles D.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(maximum 200 words)*

One problem an intranet planner faces is that it takes too long to research the subject. Initially, the intranet planner needs to get the "big picture" -- not implementation details. This thesis will help the reader quickly grasp intranet concepts, terminology, and major issues, in order to save time in formulating an effective strategy. The thesis defines Internet, intranet, and extranet, from physical and organizational viewpoints, and introduces the issues discussed in later chapters. The control issue is shown to be the common theme in debates about centralized versus distributed computing, thin versus fat client, closed versus open access, supplier push versus user pull, and management control versus employee empowerment. There is a discussion of what Web technology does well, how to integrate it with existing technology, Java, and top-down versus bottom-up intranet development. Network architecture and firewalls are discussed, as well as, network security threats and what can be done to counter them.

14. SUBJECT TERMS	15. NUMBER OF PAGES
Intranet, Planning, Guide	129
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

Approved for public release; distribution is unlimited

A PRACTICAL GUIDE TO INTRANET PLANNING

Charles D. Kleinhans
B.S., Purdue University, 1968

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SOFTWARE ENGINEERING

from the

NAVAL POSTGRADUATE SCHOOL
September 1997

NPS Archive
1997.09
Kleinhans, C.

DUDLEY KNOX LIBRARY
NAVAL POSTGRADUATE SCHOOL
MONTEREY CA 93943-5101

DUDLEY KNOX LIBRARY
NAVAL POSTGRADUATE SCHOOL
MONTEREY CA 93943-5101

ABSTRACT

One problem an intranet planner faces is that it takes too long to research the subject. Initially, the intranet planner needs to get the "big picture" -- not implementation details. This thesis will help the reader quickly grasp intranet concepts, terminology, and major issues, in order to save time in formulating an effective strategy. The thesis defines Internet, intranet, and extranet, from physical and organizational viewpoints, and introduces the issues discussed in later chapters. The control issue is shown to be the common theme in debates about centralized versus distributed computing, thin versus fat client, closed versus open access, supplier push versus user pull, and management control versus employee empowerment. There is a discussion of what Web technology does well, how to integrate it with existing technology, Java, and top-down versus bottom-up intranet development. Network architecture and firewalls are discussed, as well as, network security threats and what can be done to counter them.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF SYMBOLS, ACRONYMS AND/OR ABBREVIATIONS

ATM	Automatic Teller Machine
CD-ROM	Compact Disk Read Only Memory
CGI	Common Gateway Interface
CPU	Central Processing Unit
DMZ	Demilitarized Zone
DNS	Domain Name System
DoD	Department of Defense
DQDB	Distributed Queue Dual Bus
FTP	File Transfer Protocol
GB	Gigabyte
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
IEEE	Institute of Electrical and Electronic Engineers
IP	Internet Protocol
ISP	Internet Service Provider
ISV	Independent Software Vendor
IT	Information Technology
LAN	Local Area Networks
MAN	Metropolitan Area Network
MB	Megabyte
NC	Network PC
NetPC	Network PC
PC	Personal Computer
PGP	Pretty Good Privacy
PGP/MIME	Pretty Good Privacy/Multipurpose Internet Mail Extensions
PIN	Personal Identification Number
PPP	Point-to-Point Protocol
RAM	Random Access Memory
RAS	Remote Access Service
SDRIW	San Diego Regional Info Watch
SLIP	Serial Line Internet Protocol

SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSL	Secure Sockets Layer
S/MIME	Secure Multipurpose Internet Mail Extensions
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VTC	Video Teleconferencing
WAN	Wide Area Network
WWW	World Wide Web (or Web)

I. INTRODUCTION

A. BACKGROUND

Today most organizations either have an intranet or are in the process of creating one. Because of the intense interest in intranets, there is already a wealth of information written about them in books, in magazine articles, and on numerous Web sites. If fact, 94 intranet-related Web sites were bookmarked during the literature search for this thesis. One problem an intranet planner faces is that it takes too long to research the subject.

One solution is to provide a guide that gives the reader the "big picture" about intranets by succinctly presenting the important concepts, issues, strategies, and terminology. Such a guide should be useful in planning a new intranet or in analyzing an existing intranet. It should provide references to other sources, if more detailed information is needed. This thesis is intended to be such a guide.

B. OBJECTIVES

The purpose of this thesis is to solve a real-world problem -- providing the intranet planner with a practical guide that saves time and effort over doing a literature search or "surfing the Web." The objectives of the research are:

1. Discuss Important Concepts, Issues, Strategies

Provide a conceptual understanding of intranets as a basis for more technical knowledge. Discuss important issues to help the reader make better decisions. Discuss the strategies that are commonly used in successful intranets.

2. Define Important Terminology

Define important terminology so the reader can communicate on a technical level with others in the field. Technical terms used in this thesis are listed in the Glossary.

3. Provide References to Other Information Sources

While a plan is being developed, it is the major decisions that count. Once implementation has started, the reader will want access to a plethora of technical details to accomplish the task. Many good sources of additional information are listed in the List of References and the Bibliography. In addition, Appendix B lists the intranet-related Web sites bookmarked while preparing this thesis and Appendix C lists the Internet search engines used to find these sites.

C. THE RESEARCH QUESTION

The area of research for this thesis is *Intranets*. The primary research question is: *What are some of the important*

issues that should be considered when planning an intranet?

Subsidiary research questions are:

(1) What are some of the important concepts and terminology related to intranets?

(2) What strategy should be employed for an intranet development?

D. SCOPE, LIMITATIONS AND ASSUMPTIONS

1. Scope

The scope of this thesis is intranet-related concepts, terminology, issues, and strategy that should be considered when planning an intranet.

Because an intranet, an extranet, and the Internet are related parts of the information system and use the same technology, all three are discussed. The relationships between them and the roles each of them plays helps put intranets in context for a better understanding of just what an intranet is.

In this thesis an intranet is viewed as everything needed to perform the function of an intranet. This includes software (Web client, Web server, CGI, Java), protocols/standards (HTTP, HTML, TCP/IP, Ethernet™), and the networking infrastructure that is used (firewall, routers, backbone, hubs, cables, etc.), and people.

In order to stay at a conceptual level of planning, the technical details needed to implement an intranet are left to other sources.

2. Limitations

This thesis was limited by the time available for researching the volume of published information. Like the person who will be using this guide, the problem is not a lack of information, but finding the right information, when there is too much information available. Since time did not permit a comprehensive review of all the published information, the literature review should be considered a cross-sectional sample of what is available.

3. Assumptions

It is assumed that the reader may be a project manager charged with developing an intranet for an organization. The reader may also be a higher level manager who wants to understand intranets conceptually, to know what issues to be concerned with, and to understand the jargon associated with intranets.

E. LITERATURE REVIEW AND METHODOLOGY

During the research phase of this project, reading material consisted of intranet-related books, magazine and journal articles, and Web documents. The Preliminary Bibliography from the Thesis Proposal was used as a starting point.

To find useful, intranet-related Web sites, the following method was used:

(1) Compile a list of Internet search engines (see Appendix C for a list of these search engines).

(2) With each search engine, search for the word *intranet*. This typically yielded thousands of hits ranked by relevance.

(3) Look at the first twenty (most relevant) Web sites listed in the search results.

(4) If the information found at the Web site was judged to be of potential use in the thesis, the location was saved as a Web browser bookmark (see Appendix B for a list of the Web sites that were bookmarked). In general, sites containing white papers and tutorials about intranets were saved, while commercial sites merely promoting their products were not.

F. DEFINITIONS AND ABBREVIATIONS

Definitions of technical terms used in this thesis are listed in the *Glossary*. Abbreviations are listed in the *List of Abbreviations, Acronyms, and Symbols* just before this chapter (pp. xiii).

G. OVERVIEW/OUTLINE OF THE DEBATE

This section presents an overview of some basic concepts and terms related to intranets.

1. Physical View of a Network

In this view a network is composed of hardware components, such as computers, cables, hubs, bridges, backbones, routers, gateways, firewalls, etc. Figure 1 shows a physical view of a network. It is a simplistic view of *the Internet* interconnecting *intranets* belonging to several different organizations.

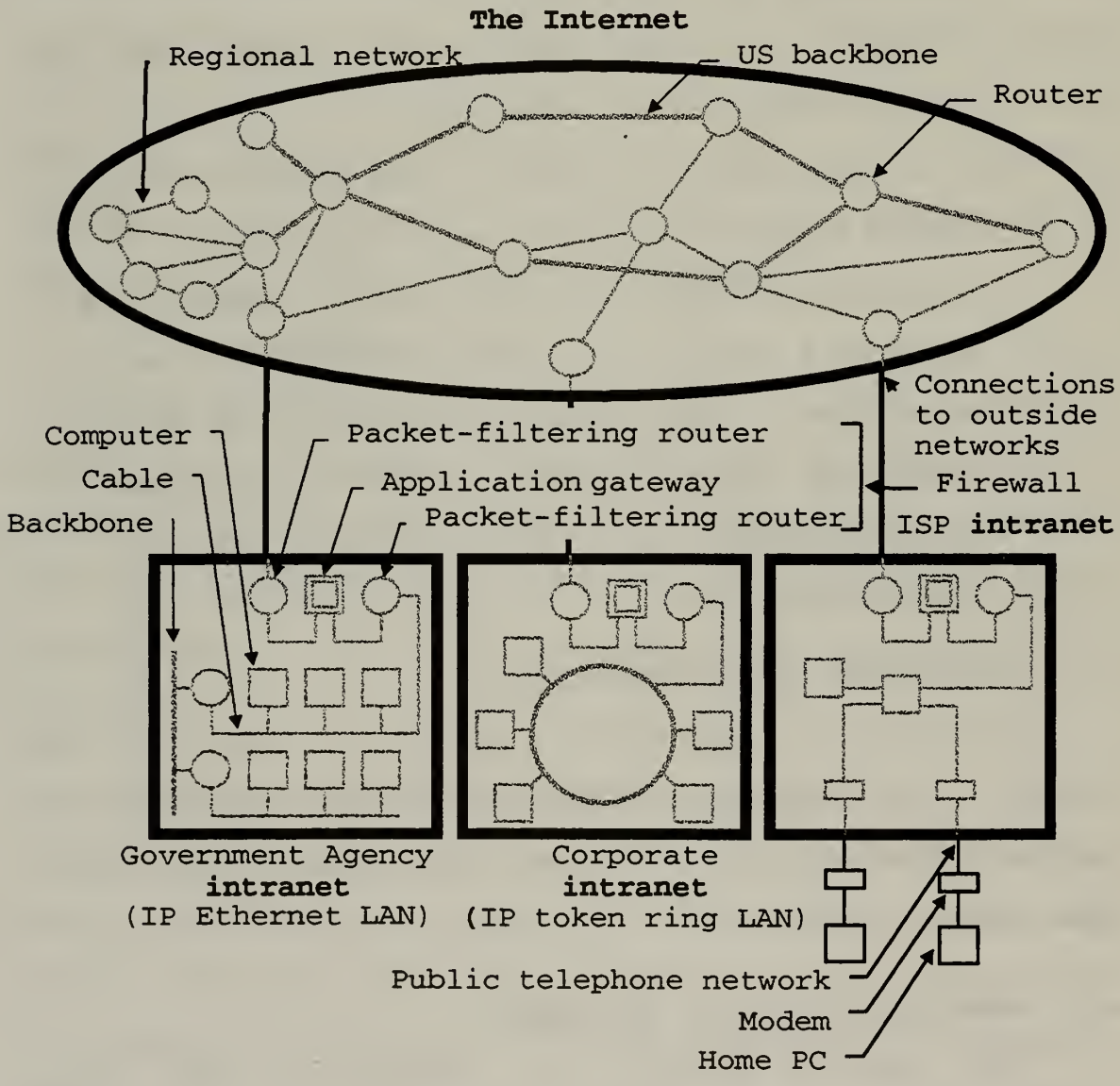


Figure 1. Physical View of a Network. After (Tanenbaum, 1996, Gibbs and Smith, 1993)

2. Organizational View of a Network

In this view a network is composed of people playing various organizational roles. The *intranet* has employees. The *Internet* has customers. The *extranet* has suppliers, distributors, dealers, business partners, and anyone else with privileged access to the organization's private network. Figure 2 shows an organizational view of a network.

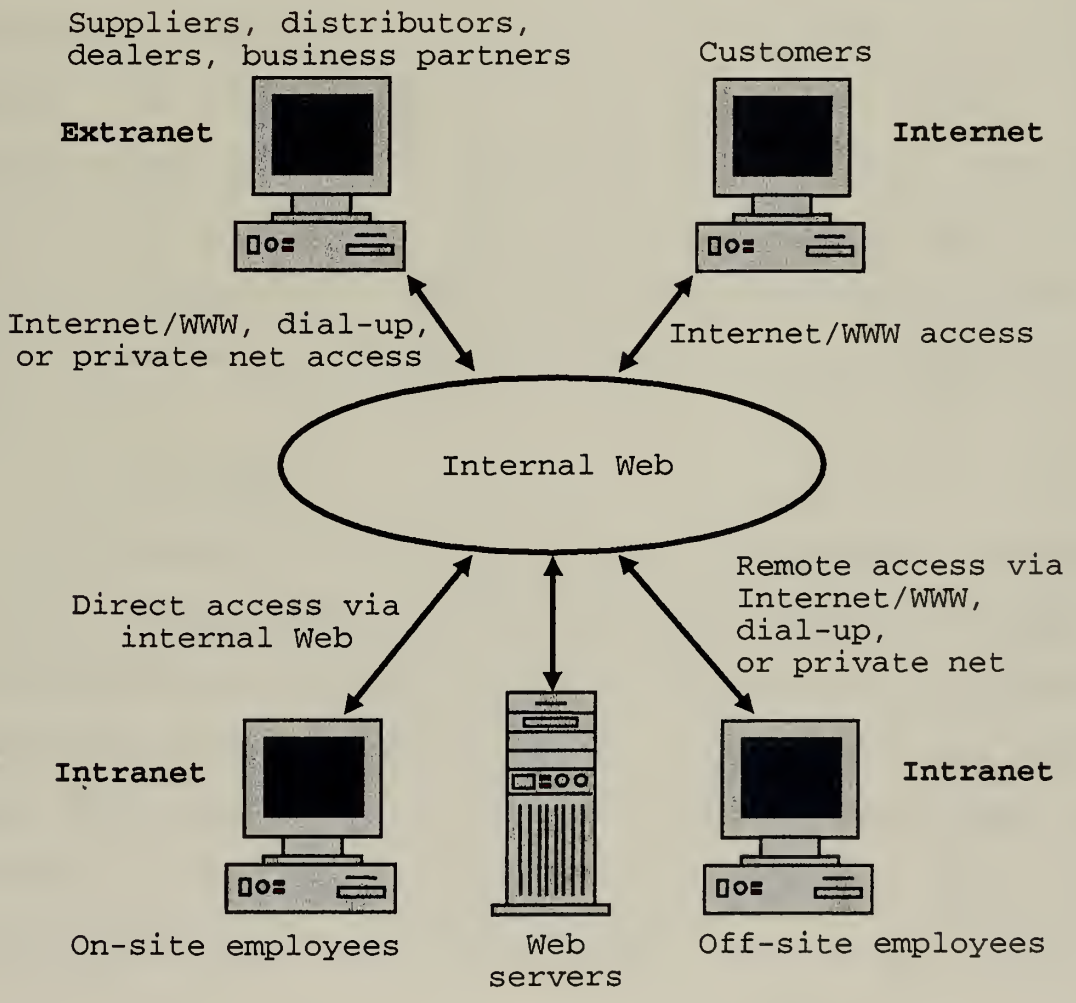


Figure 2. Organizational View of a Network. After (Bernard, 1996)

3. Internet and [The] Internet

An *internet* (internetwork) is a network that *interconnects* other networks (e.g., Local Area Networks (LANs) at different organizations, as shown in Figure 1).

The *Internet* (spelled with a capital I) is the worldwide interconnection of networks operated by government, educational institutions, commercial organizations, non-profit organizations, and even private parties. As Carroll (1996) points out, the Internet is a worldwide collection of computers and networks that have agreed to interconnect and communicate using the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. No one owns or maintains the Internet as a whole. Instead, each organization maintains and enhances a small piece of the Internet that it owns, for the benefit of all.

4. Intranet

An *intranet* is an enterprise-wide, internal, private network. It is the part of the network inside the firewall. Intranets are considered to be an application of Internet technology within an organization (i.e., TCP/IP and World Wide Web protocols). Unless otherwise specified, an intranet will be considered synonymous with an organization's private, internal Web.

5. Extranet

An *extranet* gives suppliers, distributors, dealers, and business partners restricted access to an organization's private network. An example of this might be when suppliers are able to access their customer's inventory database to automatically re-supply stock when it gets low and when it is needed for a "just-in-time" inventory system. Users of the extranet would not have access to everything on the intranet, only the data needed, and access would normally be password-protected, since the data accessed is not usually for public consumption.

6. The World Wide Web (WWW)

The World Wide Web (the Web) is a world wide, virtual network of Web servers and Web clients. The Web servers serve HTML-formatted documents using the Hypertext Transfer Protocol (HTTP) for communication between client and server. The documents are viewed with a Web browser (Web client software), which decides how to display the document, based on the embedded HTML markup tags.

The Web has become the de facto world wide standard for information delivery. Some of the reasons are:

a. Easy to Use

The Web browser displays the document and highlights links to other documents. A single mouse click on a link sends a request for that document over the network

(Internet) to the server that has the document, which could be any Web server in the world. Seconds later (usually), the requested document is delivered to the requesting browser and displayed.

b. Interoperable

Web browser software is available for Windows, Macintosh (Mac), and UNIX platforms, which means that everyone in the organization can use a Web browser to view documents, regardless of their computer. Also, by connecting the Web server software to databases or existing corporate applications using middleware, all the corporate data can become accessible with a Web browser. This provides a way for the organization to integrate all the various legacy technologies still in use with a standard user interface (the Web browser).

c. Multimedia

Web documents can not only display text, but graphic images, sound, video, and animation.

d. Java

If a Web document contains embedded HTML tags pointing to a Java applet, the applet will be downloaded and executed by the Java interpreter that is built into the browser. This enables the Web document to "bring along" whatever software may be needed to view the document

(similar to browser helper applications). This also makes it possible to download software on demand rather than having to store it all on the personal computer.

7. Protocols

As Tanenbaum (1996) points out, to reduce design complexity, networking software is designed as a series of layers or levels. At the top is the application layer. At the bottom is the software that deals directly with the hardware (or physical medium). The purpose of each layer is to provide services to the higher level software that calls (invokes) it. If the interfaces between the layers are well defined, all the implementation details do not have to be known to understand the software -- only the interface has to be known. It also means that a software layer can later be replaced with a better implementation, as long as the interface does not change.

An example of this kind of software is the TCP/IP protocol suite. If two computers are to communicate across the Internet, they both must install software that implements the TCP/IP standard (usually call a TCP/IP protocol stack). As Tanenbaum (1996) describes it, Layer n on one machine carries on a conversation with Layer n on the other machine, with the rules of this conversation being known as the Layer n *protocol*.

Tanenbaum (1996) shows the layers and associated protocols for the TCP/IP protocol stack in his book. Table 1 below shows a similar layer to protocol mapping.

Application Layer	TELNET File Transfer Protocol (FTP) Simple Mail Transfer Protocol (SMTP) Domain Name System (DNS)
Transport Layer	Transmission Control Protocol (TCP) User Datagram Protocol (UDP)
Network Layer	Internet Protocol (IP)
Physical + Data Link Layer	LAN protocols (e.g., Ethernet) others

Table 1. TCP/IP Layers and Protocols. After (Tanenbaum, 1996)

8. Firewalls

A firewall is a network device that acts as a barrier between an organization's intranet and the Internet. It is intended to be like a one way mirror, letting requests from the intranet go out to the Internet, but denying unauthorized public access (from the Internet) to the intranet. A firewall is usually a packet-filtering router, a proxy server, or a specialized firewall product (hardware and software).

A packet-filtering router works by filtering incoming and outgoing packets based on the source and destination IP address (network address of the computer) and port number

(which identifies the type of service - e.g., Telnet, FTP, or WWW).

A proxy server acts as a buffer between the intranet and the Internet. For instance, an outgoing request for a Web document goes to the proxy instead of directly to the Web server. The proxy, in turn, forwards it to the Web server. When the Web document is received, it is cached by the proxy and then sent to the original requester. Subsequent requests to the same Web site are downloaded from the cache instead of going out to the Internet again. This enhances network performance in addition to enhancing security.

Firewalls will be discussed in greater detail in the chapters on network architecture and network security.

9. Client-Server

The predominant type of network today is based on the client-server model. The reason is that the price/performance ratio for small computers is much better than for larger computers. As Tanenbaum (1996) points out, mainframes are roughly ten times faster than personal computers, but they cost roughly a thousand times more. Figure 3. Shows an example of a client-server network with a number of clients (personal computers) sharing one or more servers and one or more network printers.

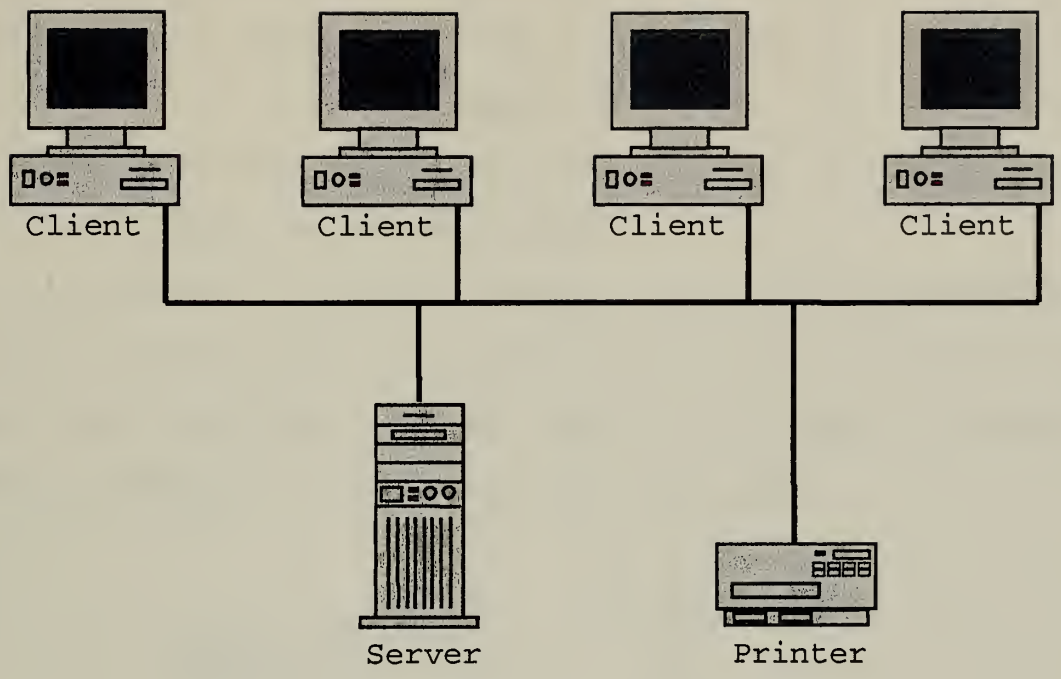


Figure 3. A Client-Server Network.

Client-server application software is split into two parts, the *client* part and the *server* part. For example, on an internal Web, the servers are running Web server software (e.g., Microsoft Internet Information Server™) and the clients are running Web client software (e.g., Netscape Navigator™). There are different ways to split the functionality of an application between the client part and the server part, with optimizing network performance being one of the major criteria in that decision. Typically, the client (*front end*) has the user interface functions while the server (*back end*) has the database access and networking functions. Depending on the amount of functionality in the client, it may be called a *thin client* or a *fat client*. The same terminology is also applied to personal computers. A

conventional PC, where application software is stored and executed on the PC, is called a *fat client*. A *diskless workstation* or *network computer*, where the application software is stored on the network, is called a *thin client*.

10. Local Area Network (LAN)

A LAN is a computer network that connects computers (hosts) located within a limited area, such as those in the same room, building, campus, ship, or aircraft. Figure 4 shows an example of two common LAN topologies.

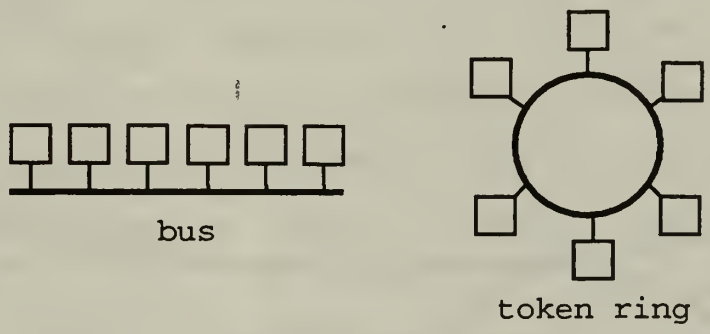


Figure 4. Common LAN Topologies.

Two of the most common types of LAN are the Ethernet™ LAN and the token ring LAN. Both use a broadcast switching technique, which means that when one host transmits, all hosts hear the transmission. An Ethernet™ LAN, specified in the IEEE 802.3 standard, uses a bus topology and operates at 10 or 100 Mbps. If more than one host transmits at the same time, a collision occurs and each host involved in the collision retransmits later, after a random waiting time. A token ring LAN, specified in IEEE 802.5, uses a ring topology and operates at 4 or 16 Mbps. Since a token

(indicating which host is allowed to transmit) is passed around the ring to coordinate transmissions, collisions are avoided.

11. Metropolitan Area Network (MAN)

A MAN is a computer network that interconnects LANs located within a metropolitan area. A local cable TV network is an example of a MAN. A new MAN standard is called Distributed Queue Dual Bus (DQDB), specified in IEEE 802.6. It uses a dual bus topology and operates at 150 Mbps. DQDB uses a broadcast switching technique, but avoids collisions by having hosts queue up requests to transmit. (Tanenbaum, 1996) Figure 5 shows an example of a MAN topology using DQDB.

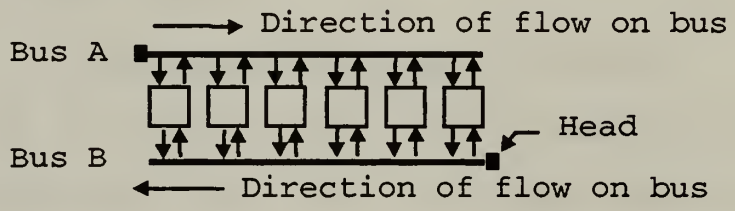


Figure 5. MAN Topology Using DQDB. After (Tanenbaum, 1996)

12. Wide Area Network (WAN)

A WAN is a computer network that interconnects LANs and host computers located over a wide area, such as a country or continent. A single organization with widely dispersed offices may use a WAN to link together its offices. Note that a subnet contains only routers and transmission lines - no hosts. Figure 6 shows a WAN connecting two LANs.

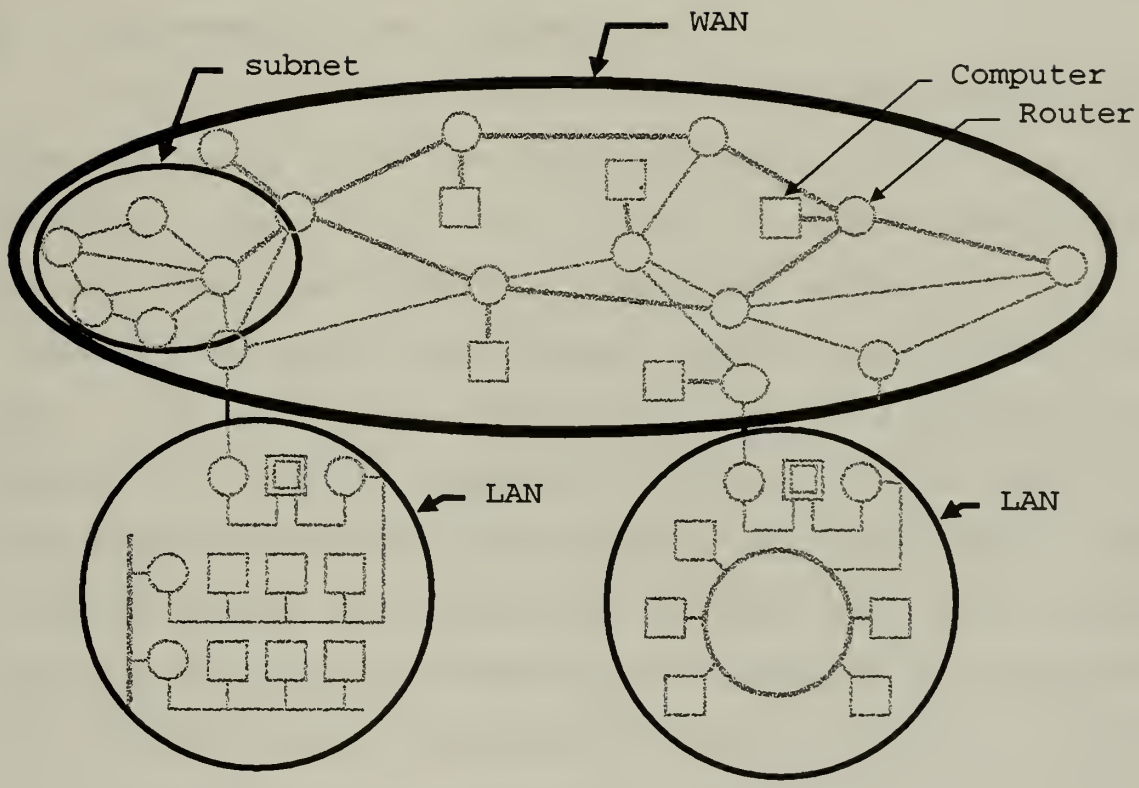


Figure 6. A WAN Topology. After (Tanenbaum, 1996)

II. MAJOR ISSUES

This chapter briefly introduces some of the major issues that an intranet planner needs to address. The following chapters discuss these issues, with a separate chapter for each issue.

A. THE CONTROL ISSUE (CHAPTER III)

This is an issue that is not just technological, but also has to do with the organizational culture. On the technical level, the issue is many faceted: centralized versus distributed computing, thin client versus fat client, closed access versus open access, supplier push versus user pull. On an organizational level it is a question of whether it is the management control or the employee empowerment philosophy that permeates the organization. An intranet planner should consider the pros and cons of each approach and be aware of whether the approach is consistent with the prevailing organizational mindset.

B. PLANNING THE INTRANET (CHAPTER IV)

This chapter will start with a discussion of the kinds of things Web-based intranets do well. This will give the intranet planner a perspective on where he or she should be heading with this technology. A related, philosophical planning issue is whether to pre-plan the enterprise structure or to let it grow and impose structure after-the-

fact. Integration of Web technology with existing technologies and Java are also discussed in this chapter.

C. NETWORK ARCHITECTURE (CHAPTER V)

This chapter will begin by discussing how to use a firewall to segment the network into the Internet, the intranet, and the perimeter net (firewall with three interfaces). The rest of the chapter will discuss firewalls in greater detail.

D. NETWORK SECURITY (CHAPTER VI)

At a recent conference, the message that summed up one speaker's talk (with personal experiences and statistics to back it up) was: The threat is real! You are at risk! (Tom Perrine, San Diego Supercomputer Center, San Diego Regional Info Watch Second Annual Network Security Symposium). The basic, network security issue is: How can the intranet be protected from the security threats and not excessively impact the sharing of information, workgroup collaboration, and employee productivity? This chapter provides some answers.

III. THE CONTROL ISSUE

In this section a number of issues are discussed: centralized versus distributed computing, thin client versus fat client, closed access versus open access, supplier push versus user pull, management control versus employee empowerment. Notice that there is a common theme running through all of these debates, which is: Who is in control? Is it the central planners on staff in the organization's Information Technology (IT) department or is it individual employees, project groups, or functional groups? Which side of the issue is favored probably depends on to which group the reader belongs and which factors are considered most important. The discussion begins with a historical overview that reveals long-term trends related to the control issue.

A. A HISTORICAL OVERVIEW

1. The Mainframe-Supercomputer Era

In the early days of computers (the 1950's), a computer was so expensive that only the military, a university, or a large corporation could afford to own one. Programs were written in machine language, so they were exceedingly difficult to write. Later, assembly languages (second generation languages) made programming far easier.

In the 1960's, most organizations had a computer for the entire organization. The computer was put in a

protective "glass house", where it was cared for by system administrators, computer programmers, and computer operators. High order languages (third generation languages) made programming far easier. When terminals were introduced, a program could be run and results obtained right away, instead of having to submit a deck of keypunched cards for an overnight batch job.

In this centralized environment, users were at the mercy of the IT staff. Users wanting applications written to help them with their jobs often had to wait years for the IT staff to do the programming that was needed. One advantage, however, was that central control made administration and security much easier. Everything was in one place, controlled by one group, and was inaccessible to the outside world. The administrator could dictate corporate standards, create and delete user accounts, force users to change their passwords, backup the data to magnetic tape every night, and so on. The IT staff was in control and employees just had to make the best of it.

2. The Mini-Computer Era

Next was the mini-computer revolution (in the 1970's). The computer had shrunk from the size of a room to the size of a cabinet and performance had increased. The price had dropped to the point where any department or division could own its own computer and use it for its own purposes. The central mainframe and the IT staff were still around, but

dealt mostly with mission-critical, enterprise databases, payroll programs, etc. The mini-computer was usually used by engineering departments for scientific or manufacturing purposes. This was the beginning of distributed computing, since there were now multiple computers under the control of different groups.

3. The PC Era

Next was the Personal Computer (PC) revolution (in the 1980's). Now computers had shrunk to a size that would fit on a desktop and performance had increased. They were inexpensive enough that every person in the organization could have a computer on their desk to do their work. Now distributed computing meant thousands of computers. The central computer and IT staff were still around, and so were the department computers, but now employees had their own computers. They were empowered. They could go out and buy whatever software they thought would help them do their jobs. They could create their own letters instead waiting for the secretary to get to their letter in the typing In-Basket. They could use a computer without having to know how to write a computer program.

There were some problems though. Because so many people were making their own choices, there were hardly any standards, except de facto standards like WordPerfect word processors or Lotus 1-2-3 spreadsheets. Some people bought Macs, some bought PCs, while the departments still used UNIX

machines. People had a difficult time sharing data because of the multitude of incompatible, proprietary file formats in use. Since employees were now system administrators for their own PCs, they needed technical support from the vendors and from their own organization. In spite of the problems, users were never happier, because they were finally in control. However, the IT people and management thought costs were out of control and were upset by all the chaos caused by the lack of standards. Even though PCs could be purchased for a few thousand dollars, it has been estimated that the support cost was close to $10,000 per year per user.

4. The Networking Era

The next revolution (in the 1990's) was networking. PCs came with Ethernet™ cards and the organization had a plethora of servers that employees had access to via the corporate Local Area Network (LAN). Data or applications on servers could be shared by everyone in the organization. Distributed client-server software was the way things were done. The control pendulum had begun to swing back, with IT reasserting itself, establishing standards, and buying site licenses for software. The corporate standard was usually Microsoft Office™ running on a Windows™ or Macintosh™ operating system.

Within the last few years organizations have interconnected their corporate LANs using the Internet and

the World Wide Web has made the Internet easy to use. Now, it seems, every company in the world has a Web site to market its wares and do business over the Internet (i.e., electronic commerce). Even private parties can create a Web site on their home computer. As popular as the Internet is, about 10 times as much money is being spent by organizations in creating intranets (internal Webs). After that, expect the intranets to extend outside the organization to extranets that include suppliers, distributors, dealers, and business partners. Distributed computing now encompasses millions of interconnected computers.

5. Megatrends

This historical overview reveals several long-term trends.

a. Computer Hardware

Computer hardware is always becoming smaller, cheaper, faster, and able to run larger programs. The physical size of a computer system has gone from room size mainframe to notebook PC. Computer system prices have dropped from millions of dollars to a few thousand dollars. Processor speed doubles about every 18 months. At this rate, the computer bought today will be obsolete within five years. The amount of memory and hard disk storage is also continuing to increase. An 80286 based PC might have come with 8 MB of RAM and a 40 MB hard drive. Today a Pentium™

based PC might come with 32 MB of RAM, a 3 GB hard drive, and a CD-ROM drive. The ever increasing speed and capacity of computer hardware makes it possible to run ever larger, more complex software, that does what was not practical to do before.

b. Computer Software

Computer software is always becoming larger, more complex, and able to do more (increasing functionality). This increasing functionality is the result of writing additional code, which makes the software larger and more complex than before. This, in turn, means the software requires more disk space for storage and more memory for execution. The ever larger software demands ever increasing speed and capacity from computer hardware in order to execute at an acceptable level of performance.

Much of the increasing functionality of software is a result of making the software more intelligent and easier to use. The historical trend for the human-computer interface has been away from machine language and towards human language, making the computer easier to program and easier to use. The graphical user interface of today's software is only practical with today's computers, because the performance would have been unacceptably slow with earlier computers.

c. Computing Model

The historical trend has been away from the centralized computing model and towards the decentralized (distributed) computing model. In the 1950's and 1960's, an organization may have only had a single computer for the entire organization. Later, when mini-computers became available, the number of computers operating in the organization may have been from several to tens of computers. By the time every employee had a desktop PC, there may have been thousands of computers in a single organization. The distributed computing model became the inevitable result of networking these thousands of computers together so employees could share data and work together. The Internet and World Wide Web are a distributed computing model encompassing millions of computers.

Notice that every aspect of computing has become distributed. Not only are data, applications, and processing power distributed over thousands of computers in an organization, but so are the responsibilities for system administration and security. Each individual creating data on the PC decides whether the data should be shared or kept private. Each PC user may also do such system administration tasks as changing the computer configuration, performing backups, installing new software, etc. Often the organization will have a support group to assist users with such tasks.

Also notice that each new level of technology did not do away with the previous installed base. The mainframe computer running enterprise level applications and databases and the IT support staff is still there. The department and division level servers for engineering and manufacturing are still there also. Instead, just as the supply/demand curve in economics would suggest, as the price of computer systems continued to drop, more computers were purchased and an ever larger portion of the population was able to own one.

d. Management Control versus Employee Empowerment

Along with the shift from the centralized computing model to the distributed computing model was a shift from centralized authority (management control) to distributed authority (employee empowerment).

During the first half of the 1990's, the United States went through a period of downsizing. This happened in the government and the military, as well as, in corporate America. The government tried to follow what corporate America was doing. The military was forced to downsize through budget cuts, but tried to maintain its effectiveness as best it could. There were major changes. The military services realized that truly joint programs and operations and interoperable systems were now a necessity. There was a Department of Defense (DoD) wide corporate information management program. The military services adopted the use

of commercial off-the-shelf technology in military systems and did away with military specifications and standards.

Corporations tried to be more competitive by reducing costs -- specifically labor costs. The idea was to do more with less (i.e., to provide better products and services with fewer people). The strategy was to reengineer business processes and to support the new, streamlined business processes with computer technology to produce the same output with fewer people. The downsizing resulted in a reduction in overhead and middle management and a distribution of those responsibilities to the remaining employees. Employee empowerment initiatives gave employees more opportunity to participate in management decisions and more computer technology to help with the extra work resulting from staff reductions. Technology did help to a degree as applications like email, file servers, and workgroup software (like Lotus Notes™) helped employees communicate better and work together better than before.

e. More on these issues

The previous discussion has been about historical trends on these issues. In the rest of this chapter the pros and cons of each issue will be discussed.

B. CENTRALIZED VERSUS DISTRIBUTED COMPUTING

Table 2 compares the centralized computing model and the distributed computing model.

Characteristic	Centralized Computing Model	Distributed Computing Model
Description	One computer shared by many users	Many, interconnected computers, distributed throughout the organization. Each computer may be stand-alone or shared.
Administration	Simple. One person or group in charge of the computer.	Complex. Different persons or groups in charge of different computers.
Security	Simple. All data in one place. If compromised, all data is vulnerable. Typically, security is a priority and highly skilled people are in charge of security.	Complex. Data is distributed, so security involves many different computers and many different people. Only some of the data compromised in a single incident. A compromise more likely since not all of the people in charge are highly skilled and some computers are not well protected.
Cost	Hardware and software much more expensive.	Hardware and software much less expensive. Higher level of administrative support needed.
Employee satisfaction	Employees less satisfied because they have no direct control.	Employees more satisfied because of greater autonomy and control.

Table 2. Comparison of Centralized Versus Distributed Computing.

C. THIN CLIENT VERSUS FAT CLIENT

When PCs are interconnected via networks, there are two ways of thinking about this. One way is to consider the PC network capable, with access to other computers whenever

there is a need to communicate with them or share data. The PC is powerful, but complicated, and employees are still in control and empowered. This is the Microsoft and Intel view of a PC. Since the PC needs enough disk space and memory to accommodate applications and data, it may be called a Fat Client. A slimmed down version, designed specifically for business, is called a NetPC. It has less memory and is not customizable by users, which reduces administration costs.

Another way of looking at the relationship between the PC and the network is to consider the entire network *is* the computer and the PC is just a client that accesses it. In this case, a much slimmer, less expensive PC, or thin client could be used. Applications would run on a server, not the PC. The user interface would be a Web browser. There would be less memory, and the hard disk would be optional, but a hard disk is not really necessary, right? Now, someone else in the organization is the system administrator for the PC and the other PCs like it. This is the Oracle and Sun view of a Network Computer (NC). They say the NC will cost about $500.

The idea of a thin client is to make the PC less expensive to own. It will be less expensive to purchase because it will not have frills, like the hard disk. The PC will be less expensive to maintain because it eliminates the need for thousands of PC users to act as system

administrators for their PCs, installing software upgrades, etc.

The idea of a thin client is really attractive to management and IT folks looking for a way to reduce costs, implement standards, and get control of their network. For instance, the organization can buy hundreds or thousands of identical, inexpensive PCs for employees and buy site licenses for the enterprise standard software. The software would only be installed on the organization's servers, eliminating the need for each PC owner to purchase and install each software upgrade that comes along. Furthermore, there would be minimal variations in PC hardware and everyone would automatically use the same version of the software, eliminating incompatibility problems and reducing support costs.

The idea of a thin client may not be welcomed by employees, who do not feel so empowered when they lose their ability to choose the hardware and software they use or even to tailor their PC to suit their needs. The one PC fits all philosophy does not account for the fact that users vary considerably. Some may only need to use corporate applications, while others need high performance machines or need to run software other than office suites. There could be other negative consequences. What happens to network performance when applications and data are being downloaded to thousands of PCs? Network downtime is much more serious

when users cannot continue to work autonomously as stand-alone PCs.

There are a number of other thin client variations, but the issue is still cost and control. The best alternative may be to offer users a choice of a corporate standard PC or the PC they feel they need to do their jobs.

D. CLOSED ACCESS VERSUS OPEN ACCESS

This issue is more of a security philosophy. Closed access means that the default is no access. For instance, a checking account cannot be accessed from an ATM without an ATM card and the correct Personal Identification Number (PIN). This is exactly the right philosophy to have if the primary concern is protecting the bank and the account from unauthorized withdrawals. How long could the bank keep its customers, if it could not provide this protection?

Open access, on the other hand, is where the default is to have access. Public Web sites and anonymous FTP sites are examples of open access. Here, the Web site owner wants to do everything possible to make sure the site is easily accessible, and that a purchase can be easily made. The object is to not lose a potential sale. This is exactly the right philosophy for this situation.

We might conclude then, that sometimes open access is appropriate and other times closed access is appropriate, depending on the situation. However, it is not always that

simple. Frequently there is a tradeoff. Customers should be able to easily access a Web site to check on the status of an order, for instance, without allowing others to look at private or sensitive material. Preventing a hacker from getting access to vandalize the site is also important. Whatever makes access easy, makes it easy for everyone (the good guys and the bad guys). Similarly, any security measures taken to restrict access, make it difficult for everyone to access the site. The dilemma, is to try to appropriately balance (or trade off) the desire for ease of access and the need for security. In this case, as a compromise, a password could be used to protect the site. Even better would be to find a method that gives both easy access and security, without having to make the trade off.

Most computer systems and network operating systems are set up using the closed access philosophy. This requires a system administrator to establish a new account and password before a new user can access the computer, file server, etc. These systems tend to be relatively secure, but difficult to use because of the burden of having to be administered.

In contrast, the Internet and World Wide Web, were designed with the open philosophy in mind. Anonymous FTP sites are an example of this. Web sites are open by default, so take special measures must be taken to restrict access (like adding an ".htaccess" file to the directory where the documents reside). This openness and ease with

which they can be accessed no doubt contributed to their phenomenal growth. It is also a reason why security is problematic with Internet technology (it was designed for access - not for security).

E. SUPPLIER PUSH VERSUS USER PULL

Information technologies can be categorized as supplier push or customer pull. For instance, email is a push technology. So are the telephone system and fax technology. To tell someone about something, one can pick up the phone and call, or send an email, or a fax. The supplier of the information pushes it the intended recipients. The recipient does not have much choice about whether to receive the information or when to get it. One problem with this is that the recipient can be overwhelmed with messages from all the people sending to him or her. Another problem is timing. A call could come at an inopportune time.

Web servers are considered a pull technology. Customers get the information provided only when they access the Web site. They choose when to access it. They also stay only as long as they are getting something that is worth their time. User pull is much friendlier because the recipient is in control.

Because of this, a user pull type of information delivery system is much preferred, except in special cases.

These are where it is important for the recipient to be notified or where the recipient chooses to be notified.

This situation is changing with Web technology, however. Already, flashing, animated, advertisements are being pushed at the reader when visiting certain Web sites. Soon, push technology will be added to Web server software. Use it wisely.

F. MANAGEMENT CONTROL VERSUS EMPLOYEE EMPOWERMENT

The degree of management control varies from organization to organization. A high degree of management control is appropriate for some organizations, like the military. In other organizations, such as high tech companies that depend on a creative, motivated work force, and where retention of skilled employees is important, an emphasis on employee empowerment is a better approach.

As Bernard (1996) observes, in companies where they are truly empowered, employees tend to take Web technology and run with it in all kinds of unexpected ways. He says that Web systems work best when people are given the same freedom to use the technology as they have with other applications.

An example of where the issue of management control affects Web technology is management policy on employees setting up their own Web pages. On one hand, management needs to ensure that sensitive, corporate information is not inadvertently published on a Web site accessible by the

public. Management also wants to make sure that the Web publishing privilege is not abused, for instance by serving pornographic images downloaded from the Internet. On the other hand, there is probably no better way for employees to share valuable information throughout the organization, than by encouraging them to turn their PCs into Web servers accessible throughout the intranet. Some companies make the Web publishing privilege a reward to encourage the spread of Web technology in the organization.

Management can both encourage personal Web sites and still avoid the problems. One way is by creating an Acceptable Use Policy and a certification process for publicly accessible Web sites. Finally, employees should be held accountable for how they manage their Web sites.

IV. PLANNING THE INTRANET

This chapter discusses the issue of what role Web technology should play in an organization's IT strategy. How should it be integrated with existing technology? How should it be deployed? The chapter begins with a section about the role of Web technology. After that are sections on integration with existing technologies, Java, and planning an intranet strategy.

A. THE ROLE OF WEB TECHNOLOGY

1. The Paperless Office

The concept has been around for a long time. Electronic documents, which can be converted to paper, at any time, replace paper documents. As suggested by Bernard (1996), users should be able to access any kind of computer object, transparently, across a network. Computer objects are anything that can be stored digitally. They may be documents, photographs, live video, music, programming tools, libraries, etc. Being able to do all this should save tons of paper, tons of money, and vastly improve the speed at which things happen.

2. Today's Technology

The paperless office is almost here. There are networked PCs on every desk, laptops and wireless networks for mobile computing, file servers, database servers, word

processors, and electronic mail (email). Video Teleconferencing (VTC) and electronic white boards make it possible to have meetings without travel. Groupware, like Lotus Notes™, helps groups of people work together more effectively. The Internet provides transparent access to computers anywhere in the world.

So what is missing? Until the World Wide Web came along, there was not a really easy to use, inexpensive, universal, non-proprietary, user interface (Web browser) that could act as a front end to virtually any back end application, including legacy applications.

The Web browser is called the *universal client* (or universal playback device), because it provides a standard user interface to display or play back any kind of data or to run any kind of application. Web browsers are able to natively display documents containing text and images. With helper applications, plug-ins, and Java applets, they can be extended to display any kind of data (proprietary document formats, audio, video, etc.).

3. What Web Sites Do Best

Basically, what Web sites (Web servers) do best is publish documents, distribute up-to-date, time-sensitive information, and interact with users, electronically. Users can easily get the information they want, when they want it, regardless of where the information is located.

For example, to distribute a catalog, thousands of copies would have to be printed and possibly shipped all over the country. The correct number of catalogs to print could only be estimated. Some people who want a catalog would not get one and others, who did get catalogs, would not want them. The printing, shipping, waste, and missed opportunities are very expensive. In addition, the catalog could not provide time-sensitive information that was current.

Instead, consider using the Web to deliver the catalog. When someone wants to see the catalog, they click on a hyperlink on their Web browser to deliver it.

How this happens is a little more complicated. The Web client sends a request for the document to the Web server that has the catalog. The Web server queries the back end database to extract the latest data. This is done using middleware between the Web server and the database to translate HTML to Structured Query Language (SQL). The middleware then takes the resulting data, wraps it in HTML tags, and gives it to the Web server. The Web server sends it back to the Web client that requested it for display.

The document is created on-the-fly and can contain audio or video messages or animation, as well as pictures of the products. It can also contain hyperlinks that allow the customer to find additional information, leave a message, or even place an order immediately.

4. Everything On-Line

As Bernard (1996) points out, probably only 20% of typical organization's corporate information is contained in traditional information systems (like relational databases). Web technology provides a practical way of putting the other 80% on-line. This can benefit other employees on the intranet, customers on the Internet, or suppliers, distributors, dealers, and business partners on the extranet. The way this can happen is for each employee to become a Web publisher of the information he or she works with every day.

B. INTEGRATION WITH EXISTING TECHNOLOGIES

How should Web technology be integrated? Probably the best answer is to use the Web browser as the front end (user interface) for virtually every corporate software application, including legacy applications. The Web browser is so popular today that this is almost assumed. It should be pointed out that this is not as easy as it sounds. Some applications may require a significant amount of rewriting in order to use a Web front end.

Figure 7 shows the *hardware view* of how a Web browser can be used to query data in a legacy database, as an example.

Figure 8 shows a *software view* of the same thing. Middleware is the software that integrates (glues together)

Web technology to any other technology. It is the gateway that translates one language into another (e.g., HTML to SQL and vice versa). In this case the middleware is either a Java application or a Common Gateway Interface (CGI) script, which are open (non-proprietary) standards. They are shown running on the Web server. There are also proprietary middleware choices, but these can lock the organization into certain products. Also note the Java applet running on the Web client. Although this is optional, a Java applet can be used to manage the interaction with the user. This could be displaying menus and dialog boxes, validating user input, and displaying the results in different views according to user choices.

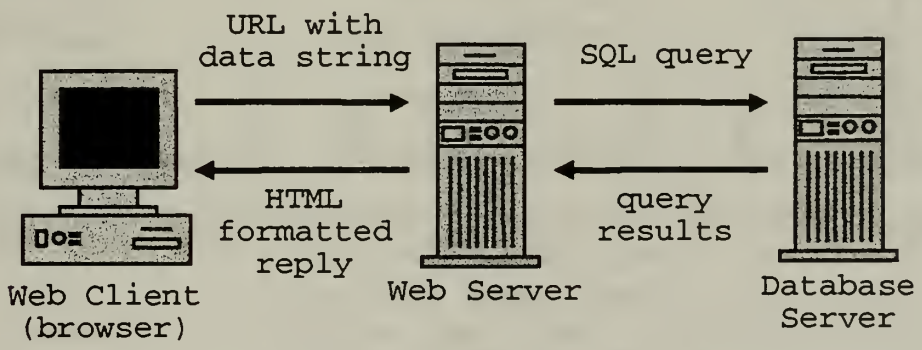


Figure 7. Hardware View of Web-Database Integration. After (Bernard, 1996)

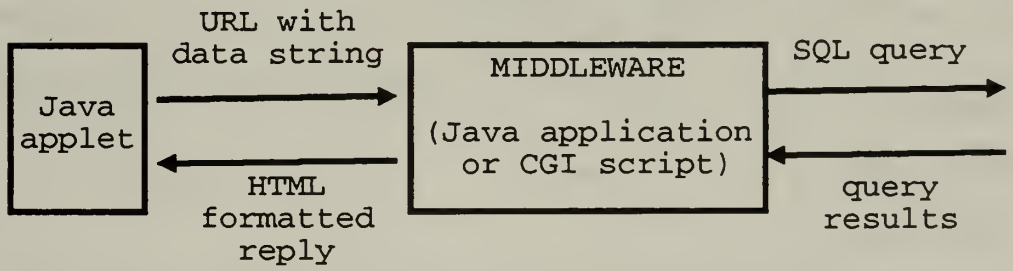


Figure 8. Software View of Web-Database Integration. After (Bernard, 1996)

C. JAVA

1. What Is Java?

This subsection summarizes ideas presented in a recent Java programming course (PRI, 1997). Java is an object-oriented programming language. Originally, it was created for Personal Digital Assistants (where available memory is small), but later adapted for use on the World Wide Web and for use as a general application programming language.

Java can be used to write applets and applications. Table 3 compares applets to applications.

	Java Applet	Java Application
Typical size	Small	Large
Compiles to	Platform-independent, byte code	Same
Stored on	Server	Server or client
Runs on	Client (downloaded with Web page and executed by Java interpreter in Web browser)	Server or client
Full access to system services (e.g., hard disk)	No	Yes

Table 3. Comparison of Java Applets and Java Applications.

Figure 9 illustrates how conventional programming languages, like C, C++, Ada, etc. are compiled for different computing platforms. In this example, three different compilers are required for the same source code. If the source code is tailored to take advantage of the particular platform, then three different versions of the source code are required, as well.

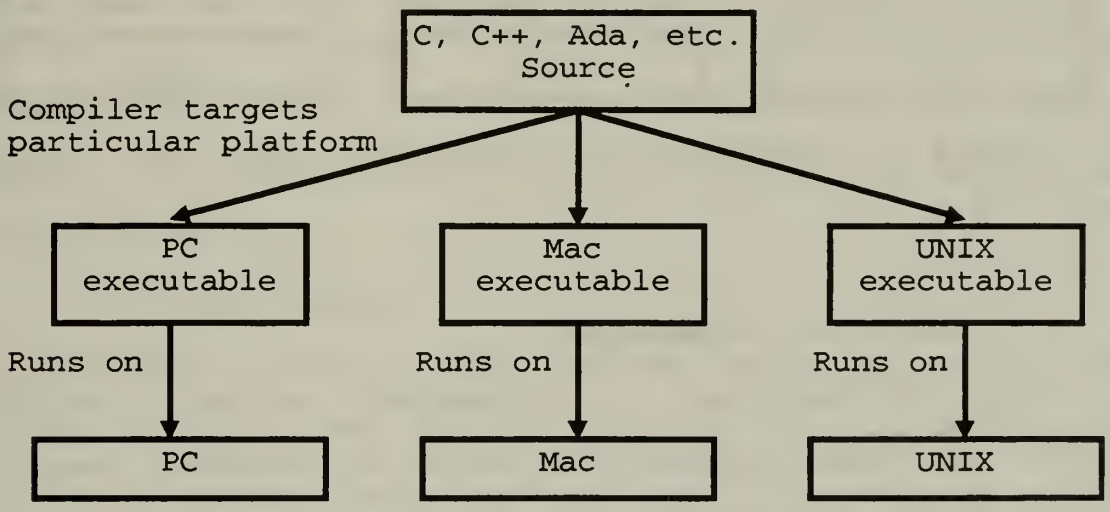


Figure 9. Compilation and Execution for Conventional Programming Languages.

Figure 10 illustrates that there is only one version of Java source and one version of Java byte code, which runs on all platforms, because the Java Virtual Machine hides the details of the platform.

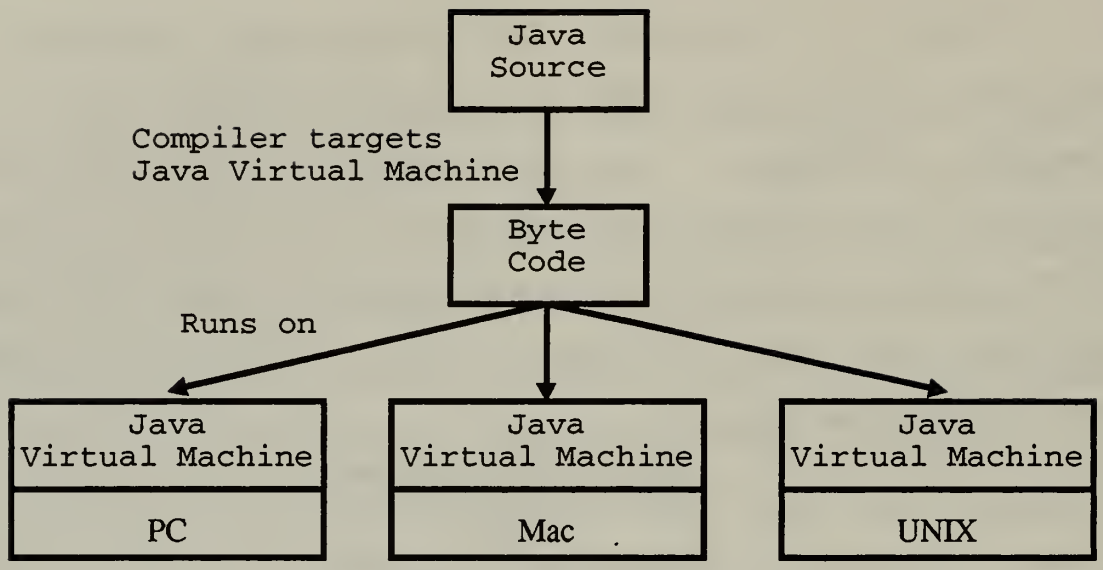


Figure 10. Compilation and Execution for Java. After (PRI, 1997)

2. Why Java Is Important

Java is important to Independent Software Vendors (ISVs), who write commercial-of-the-shelf software, because it allows them to write and maintain a single version of source code for all platforms. This makes their applications immediately portable, without the expense they now incur to target different platforms.

Another reason Java is important is that it gives Web pages the ability to run programs. When a hyperlink is clicked on a Web page, any Java applets embedded in the Web page are downloaded from the server, along with the HTML normally in the Web page, and run in the Web browser. Not only is the Web page displayed, but any program embedded in

the Web page is automatically run. For instance, if a video file was attached to a Web page, the software necessary to play the video file could be downloaded and run automatically. There is no need for the user to have a helper application to play it. As Bernard (1996) suggests, a multimedia file in a Web page comes with its own playback device.

This idea can be taken even further. As Bernard (1996) points out, potentially all applications can be delivered on demand, just in time, to the Web browser (PC, Mac, UNIX) instead of having the applications installed on individual client machines.

3. Java Security

Because a program can be run automatically on the client PC when a Web site is visited, this would seem to create an enormous security risk. Any program could be run without the user knowing it. The program could read or erase the user's hard drive, plant a virus or Trojan horse, or do a variety of mischief. Because of this potential problem, applets only run in the context of the Web page they are embedded in (inside the Web browser). They are not allowed access to system resources on the user's PC, the way a Java application is. As long as the applet is confined to the "sandbox," as it is often called, in the Web browser, it should be pretty safe to run. This limits what an applet

can do, but it seems a prudent tradeoff, considering what might happen if it was allowed to do more.

D. PLANNING AN INTRANET STRATEGY

1. Top Down or Bottom Up?

When contemplating a strategy for developing an intranet, consider the following: Historically, most internal Webs were developed from the bottom up, starting with technologically savvy individuals and spreading out from there. Web technology adoption was usually with the tolerance of management, rather than management's urging, with little help from the IT staff. In companies where employees are empowered, Web technology may spread very fast, while in companies that stifle initiative with bureaucratic control, the rate of adoption may be incredibly slow. (Bernard, 1996)

Notice that this bottom-up growth parallels the growth of the Internet. No one plans the Internet, staffs it, budgets it, or manages it. It just happens through the cooperation of millions. (Bernard, 1996)

With Web technology, probably the best strategy for developing the intranet is to give users the tools to create their own Web sites at will -- then come back after the fact and impose structure on what develops. The structure is in the form of an enterprise wide, centralized menu or

directory, with hyperlinks to all of the content. (Bernard, 1996)

There are a couple of approaches to gathering the information needed to create such a directory. One is the central registration page, where each person creating a Web site registers the Web site and provides the desired information. This ensures that the needed information can be collected in a consistent manner and provides a convenient way to certify the site (see if the site meets the organization's criteria for security, etc.). However, it will not find unregistered Web sites and the registered information can quickly get out of date.

The other approach is to use Internet Web crawlers to continuously find all the Web sites in the organization's intranet, just as they do on the Internet, and automatically update the directory. (Bernard, 1996). It must be noted, however, that Web crawlers merely follow hyperlinks they find in existing Web pages and will not find pages that do not have a link pointing to them from an existing Web page. This could significantly limit their effectiveness.

2. Two Perspectives

Of course, there are different ways of looking at an intranet development strategy. Carroll (1996) defines two, which he calls *Inductive/Proactive* and *Deductive/Reactive*. He suggests that a balanced approach, that includes both of these, is what is needed.

a. Inductive/Proactive

This approach focuses on discovering how information technology (e.g., Web based intranets) can help break traditional business rules and solve previously unperceived problems (Carroll, 1996). This might be called a solution looking for a problem, but it can help to discover creative, break-through ideas.

b. Deductive/Reactive

This approach focuses on first identifying an existing business problem and then determining the best way to solve it. This way of thinking is implicit in the systems engineering methodology. (Carroll, 1996)

V. NETWORK ARCHITECTURE

This chapter will discuss the issue of what kind of network architecture should be used for an enterprise-wide intranet. The discussion will begin with an overview of how the firewall divides the network into the Internet, the intranet, and the extranet. Next, firewalls will be discussed in greater detail.

A. THE FIREWALL, THE INTERNET, THE INTRANET, AND THE EXTRANET

1. What is a Firewall?

A firewall is a network device (hardware and software) that is placed between an organization's internal, private network and the Internet to prevent unauthorized public access to the private network. Firewalls can also protect assets, like Web servers and FTP servers, that are intended to be publicly accessed.

Essentially, a firewall enforces a network access policy (i.e., what types of incoming and outgoing access are permitted). It does this by screening incoming and outgoing traffic. Typically, outgoing traffic is permitted, so employees can access outside resources and services like Web sites, FTP sites, and Internet email, but incoming traffic is stopped by the firewall. This protects the internal, private network from a variety of outside threats.

2. Is a Firewall Really Necessary?

If an organization's network is connected to the Internet, a firewall is a necessity! No network is 100% secure, even with a firewall, and having a firewall tends to give a false sense of security, but it would still be foolish not to have one.

3. The Firewall Between the Internet and the Intranet

The simplest architecture is where the firewall is placed between the Internet and the intranet. In this case, the firewall has two interfaces.

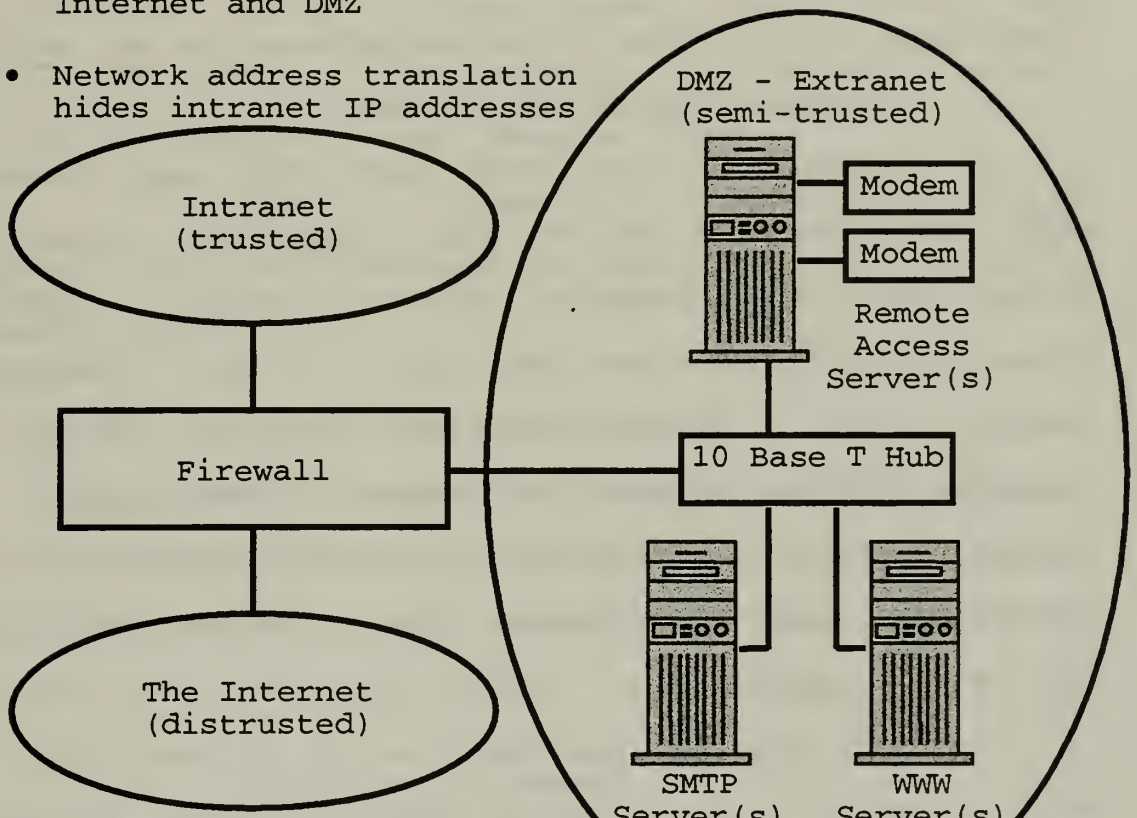
4. The Firewall Between the Internet, the Intranet, and the Extranet

A better architecture divides the network into three parts, the Internet, the intranet, and the extranet. The extranet part will be considered synonymous with what Nangle (1997) calls the Demilitarized Zone (*DMZ*). Other authors use the term *perimeter net* or *screened subnet*. Note that some firewalls only support two interfaces and therefore, cannot support this architecture.

This three-part architecture has the advantage that, even if machines in the DMZ were compromised, the rest of the intranet would still be protected by the firewall. (National Software Testing Laboratories, Inc., 1997)

Figure 11 shows an enterprise network using a DMZ that contains a remote access server serving one or more modems, an email server and a Web server.

- Intranet protected by firewall, but has access to Internet and DMZ
- Network address translation hides intranet IP addresses



- Internet access to intranet blocked by firewall
- Internet access to DMZ limited to specific protocols
- DMZ protected by firewall, but has access to Internet and intranet
- Network address translation hides DMZ IP addresses

Figure 11. Firewall Segments Network Into Internet, Intranet, and Extranet. After (Nangle, 1997)

Bernard (1996) suggests an architecture similar to that of Figure 11, which he calls a screened subnet. In this configuration, the firewall consists of two screening (packet-filtering) routers to filter traffic in both directions, with a subnet connected between the two routers.

5. Firewalls Inside the Intranet

An organization can have more than one firewall. Additional firewalls may be used inside the intranet to protect sensitive information, such as personnel records and financial records, from the rest of the organization (Nangle, 1997). In this case, the intranet side of the firewall is the side where the sensitive data resides. The Internet side of the firewall is actually the rest of the organization, and a DMZ can be used to serve data to the rest of the organization.

Firewalls are not the only way to protect sensitive data within the intranet, so an internal firewall should be considered just one alternative for protecting the data.

B. MORE ON FIREWALLS

1. Types of Firewalls

There are several different types of firewalls (discussed below).

a. Packet-Filtering (Screening) Router

The most common, but least secure and most difficult to configure type, is the packet-filtering router. It works at the network layer. It examines the source and destination IP address of each packet passing through the router. The router either forwards or drops each packet, based on user-defined rules. (Nangle, 1997)

This type of firewall is vulnerable to IP Spoofing, where the IP address is changed so that it will be allowed to pass.

b. Stateful-Inspection Device

A stateful-inspection device examines packets, like the packet-filtering router, but it remembers which connections use which port numbers and shuts down those ports when the connection closes.

c. Circuit-Level Gateway

A circuit-level gateway works at the transport layer. It authenticates TCP and UDP sessions between hosts. It terminates the session when finished with all circuits. (Nangle, 1997)

d. Application Gateway

An application gateway works at the application layer. FTP or Telnet data, for example, is examined before allowing a connection between the client process and the

server process. This is considered the most secure type of firewall. Unfortunately, application gateways are difficult to configure and require significant overhead, resulting in poor performance. (Nangle, 1997)

e. Proxy Server

Another type of firewall is the proxy server. When a host inside the firewall (intranet side) requests a service outside the firewall, the host IP address is translated to the IP address of the proxy. This hides the internal structure of the intranet from the outside world, making it more difficult for a hacker to target a specific internal host. The proxy forwards the request to the destination host and receives the reply. Finally, it forwards the reply back to the host that made the request. (Nangle, 1997)

Address translation also lets any IP address be used on the internal network and reduces the number of registered IP addresses that are needed by the organization. The connection from the proxy to the external host can be at the application layer (application proxy) or at the session or transport layer (circuit relay). (National Software Testing Laboratories, Inc., 1997)

An additional advantage is that caching on the proxy server eliminates the need to access the same external

address multiple times, which reduces the load on the network.

f. Hybrids

A firewall may use a combination of these techniques. As an example, Tanenbaum suggests a firewall configuration consisting of two packet-filtering routers with an application gateway between them. The router on the intranet side inspects outgoing packets and the router on the Internet side inspects incoming packets. If it passes the router, the packet is forwarded to the application gateway. The purpose of this arrangement is to make sure that no packet gets in or out without going through the application gateway. (Tanenbaum, 1996)

g. NetWare Firewalls

For companies with NetWare networks, IWARE Internet Suite by Quarterdeck (www.quarterdeck.com/qdeck/products/iware) and IPeXchange by Cisco Systems (www.cisco.com/warp/public/751/ij/home.html) are products that effectively act as firewalls at the TCP/IP -- IPX/SPX interface. They convert TCP/IP into SPX. This prevents TCP/IP from traveling beyond the server into the NetWare network. Use of this hybrid approach is limited to organizations with NetWare networks. (Nangle, 1997)

2. Other Things a Firewall Can Do

a. User Authentication

The firewall can also be configured to provide user authentication. User authentication would be turned on for the remote access server, but could be either on or off, as desired, for the Web server and the mail server. (Nangle, 1997)

b. Anti-Virus Scanning

Some firewall vendors also make firewall-based virus scanner software. Nangle (1997) lists Check Point Cheyenne (www.cheyenne.com) Inocu-LAN virus protection software, Trend Micro's (www.trendmicro.com) InterScan VirusWall software, and McAfee's Webshield (www.mcafee.com) software. (Nangle, 1997)

Installing anti-virus software at the firewall to scan all email, file transfers, and Web browsing traffic protects the entire organization from viruses coming from the Internet and keeps an infection from being spread to other organizations. However, even with this, individual employees can still introduce viruses into the network by bringing in infected diskettes or CD-ROMs from home.

c. Event Logging and Notification

A firewall can log information about IP addresses, services accessed, and many other details. Based on this

information, it can provide automatic notification via email or pager of potential attack, excess traffic, and operational status. This kind of notification is critical. (Nangle, 1997)

d. Encryption

A firewall can encrypt data transferred between hosts. Both hosts could be internal, or one could be internal and the other external. (Nangle, 1997)

3. Purchasing a Firewall .

The National Software Testing Laboratories, Inc. recently performed a comprehensive test of 20 firewalls. The results are shown in an August 4, 1997, Technology Report in *Government Computer News*. In these tests, some firewalls stopped unauthorized traffic and others let it through. The results of these tests are summarized below. The firewalls are listed alphabetically, by product name. A (Reviewer's Choice) after the product name indicates a Reviewer's Choice recommendation in the article. Next are the vendor name, the test platform, and three numbers in square brackets indicating their assessment of security, performance, and manageability, where 5 is excellent and 1 is poor. A comment may follow on the next line.

(1) AltaVista Firewall 1.0 for Windows NT,
AltaVista Internet Software,

Digital UNIX on Alpha,

[5, 5, 5]

(Only two interfaces -- does not support DMZ)

(2) ANS Interlock 4.0,

ANS Communications,

Modified Solaris 2.5.1 on Sun Ultra 167,

[5, 5, 4]

(Only two interfaces -- does not support DMZ)

(3) Black Hole 3.0,

Milkyway Networks Corp.,

SunOS on Sparcstation,

[2, 3, 3]

Vulnerable to TCP sequence prediction attack

(4) Borderware Firewall Server 4.0.1,

Secure Computing Corp.,

Proprietary 100 MHz Pentium,

[4, 1, 3]

(5) Centri Firewall 3.1.2,

Global Internet,

Windows NT 3.51 on Intel,

[3, 5, 3]

Vulnerable to TCP sequence prediction attack

(6) CyberGuard Firewall 3.0 (Reviewer's Choice),

CyberGuard Corp.,

SCO Multilevel Secure UNIX on Unisys,

[5, 4, 5]

(7) Cycon Labyrinth Firewall,
Cycon Technologies,
Custom BSD UNIX on Intel,
[5, 3, 4]

(8) Eagle NT,
Raptor Systems Inc.,
NT on Compaq ProSignia 200,
[4, 2, 4]
Vulnerable to TCP sequence prediction attack

(9) Firewall Plus for Windows NT,
Network-1 Software and Technology Inc.,
NT 3.51 or 4.0 on Intel PC,
[5, 1, 2]
(Only two interfaces -- does not support DMZ)

(10) Firewall-1 (Reviewer's Choice),
CheckPoint Software Technologies Ltd.,
Sun Sparcstation 5,
[5, 5, 4]

(11) Gauntlet Internet Firewall 3.2,
Trusted Information Systems Inc.,
BSD UNIX on Sun Ultra,
[4, 1, 4]

(12) Gnat Box 1.1,
Global Technology Associates,
Intel 386 or better,
[3, 3, 1]

Vulnerable to syn flooding attack

(13) Guardian,

NetGuard,

NT on 200MHz Pentium Pro,

[5, 4, 4]

(14) IBM Internet Connection Secured Network Gateway 2.2,

IBM Networking Systems,

AIX 4.2 on RS/6000,

[5, 3, 4]

Vulnerable to TCP sequence prediction attack

(15) Interceptor,

Technologic Inc.,

BSD UNIX on Intel x86,

[4, 1, 4]

(16) NetRoad Firewall,

Ukiah Software Inc.,

NetWare 4.11/IntranetWare on Pentium,

[5, 2, 3]

(17) PrivateNet Firewall System 2.0,

NEC Technologies Inc.,

Custom BSD UNIX on Intel Pentium,

[5, 3, 2]

(18) Sidewinder Security Server 3.0.1,

Secure Computing Corp.,

Proprietary 100 MHz Pentium,

[4, 1, 5]

(19) SunScreen EFS (Reviewer's Choice),
Sun Microsystems Inc.,
Solaris 2.5 on Sparcstation,
[5, 5, 4]

(20) WatchGuard Security System (Reviewer's Choice),
Seattle Software Labs Inc.,
Proprietary platform, Windows 95, NT or Linux,
[5, 3, 3]

4. Outsourcing a Firewall

Instead of purchasing and deploying a firewall for the organization, another option is to outsource to a firewall service provider. For those interested in this option, Nangle (1997) lists the following vendors:

(1) Check Point Software (www.checkpoint.com),
(2) Raptor Systems (www.raptor.com),
(3) Cyberguard (www.cyberguardcorp.com),
(4) BBN Planet (www.bbn.com/home.html),
(5) Pilot Network Services (www.pilot.net/index.html),
(6) ANS (www.ans.net)

5. Firewall Testing

It is important that a firewall be tested after it is set up, because even a minor configuration error could leave a security hole to be exploited. The process is to test the

firewall, plug the security holes that are found, and retest, until the firewall is secure. (Nangle, 1997)

One popular tool to test the firewall is the Security Administrator Tool for Analyzing Networks (*SATAN*), which is available on the Internet (http://flying.fish.com/satan/). Using SATAN can reveal the vulnerabilities that hackers on the Internet can see.

There are also commercial tools for testing firewalls. In the firewall testing by National Software Testing Laboratories, Inc. *Safesuite* from Internet Security Systems Inc. was used to launch nearly 100 attacks against each firewall. (National Software Testing Laboratories, Inc., 1997)

6. Dial-up Accounts and Firewalls

The deployment of modems is important. A Dial-up Internet account (Serial Line Internet Protocol (SLIP) or Point-to-Point Protocol (PPP) connection) made to a private account creates a back door around the firewall. (Nangle, 1997)

7. Wireless Communications and Firewalls

Tanenbaum points out a very important caveat to this whole discussion about firewalls: if some of the hosts are wireless and use radio communication, the radio transmissions bypass the firewall in both directions! (Tanenbaum, 1996)

VI. NETWORK SECURITY

This chapter will briefly examine the issue: How can the intranet be protected from security threats, without excessively impacting the sharing of information, workgroup collaboration, and employee productivity?

The chapter discusses some common security threats today and what can be done to protect against these threats. Since a comprehensive discussion of security would be too extensive to be included in this thesis, references to several security-related books are provided.

A. SECURITY THREATS

This section discusses some of the common security threats today.

1. Spoofing

Spoofing is a technique of changing the address in the IP packet to fool the firewall into thinking the packet came from an address (inside the network) that will not be blocked. Spoofing IP addresses is very easy (Carroll, 1996).

2. Snooping

Snooping is a technique of monitoring IP packets, using a device called a sniffer, to discover authentication information sent "in the clear" (unencrypted). Applications like TELNET and FTP pass user ids and passwords from the

client to the server in the clear during login (Carroll, 1996). Traffic must be encrypted to defeat sniffers.

3. Denial of Service Attack

A *mail bomb* is an example of a denial of service attack caused by repeatedly sending email to a valid user account and overwhelming system resources trying to process the incoming mail (Carroll, 1996). A denial of service attack can render a system useless by stealing Central Processing Unit (CPU) cycles and disk space from legitimate processes or by causing buffers to overflow and crashing the system.

Sending SPAM (unsolicited commercial email) is now easy to do because programs are available to send email to millions of email addresses. Mail servers shut down with the load and then angry users intentionally shut down the mail server that the SPAM is coming from. Ask yourself: Can the email server handle millions of email messages per day plus retaliation from users? (Lawhorn, J., "The Network Security Threat", *San Diego Regional Info Watch Second Annual Network Security Symposium (SDRIW 97)*, San Diego, CA, 1997)

Syn flooding is a denial of service attack where a firewall is bombarded with requests to synchronize TCP connections. This causes the firewall to respond by allocating all available buffer space to these requests and denying legitimate connections. (National Software Testing Laboratories, Inc., 1997)

TCP sequence prediction is an attack that fools applications using IP addresses for authentication (e.g., UNIX rlogin and rsh commands) into thinking that bogus packets actually came from trusted machines. (National Software Testing Laboratories, Inc., 1997)

4. Exploitation of Vulnerabilities

Bugs in software create vulnerabilities, which can be exploited. Hackers can be thought of as forming a threat pyramid: hundreds of very skilled hackers at the top; tens of thousands of moderately skilled hackers in the middle; millions of hackers at the bottom, who can use a Web browser to exploit vulnerabilities. Once a vulnerability is discovered, the very skilled hackers can attack it and create automated tools that enable less skilled hackers to exploit that vulnerability. (Perrine, T., "The Network Security Threat", *San Diego Regional Info Watch Second Annual Network Security Symposium (SDRIW 97)*, San Diego, CA, 1997)

5. Inside Threat

As an example of unintentional threats from authorized users, sailors bought CD-ROMs in the Far East and brought them back to the ship. When they played them, they brought down combat systems. (McGuire, K, *San Diego Regional Info Watch Second Annual Network Security Symposium (SDRIW 97)*, San Diego, CA, 1997)

6. Wireless (In)Security

Security for wireless ranges from weak to non-existent. Do not believe all the public relations talk from different manufacturers. If the encryption was strong, the government would not let it be exported. (Karn, P, "Security Issues in Wireless Communications", *San Diego Regional Info Watch Second Annual Network Security Symposium (SDRIW 97)*, San Diego, CA, 1997)

B. COUNTERMEASURES

This section discusses some of the things that can be done to protect against these security threats.

1. Firewalls

Packets can be filtered by IP address and port number. Allowing incoming TELNET and FTP through the firewall is asking for trouble. Put publicly accessible servers outside the firewall or in the DMZ. (Carroll, 1996)

Never install or configure a firewall on your own. Hire a qualified network administrator who has thorough training in firewall setup and who will monitor the site on a daily basis. (Bernard, 1996)

Some additional recommendations are:

- Use dedicated machines on a perimeter net (e.g., do not use a Web server as a file server)
- Send denied packets (from a proxy) to a separate machine

- Use SOCKS as a generic proxy interface
- Disable IP forwarding
- Disable NETBIOS over TCP/IP (the entire network is open)
- Disable the Guest account and the Everyone account
- Remove or rename the Administrator account

(Haack, P., "Firewalls and Proxy Services", *San Diego Regional Info Watch Second Annual Network Security Symposium (SDRIW 97)*, San Diego, CA, 1997)

2. Proxies

In addition to IP address translation to hide the internal network, proxies can log information for an audit trail. This includes client IP address, date and time, Uniform Resource Locator (URL) accessed, byte count of data passed to the client, and meta-information tags of accessed HTML files. (Carroll, 1996)

3. Dialup Networking

Dialup networking is one way to provide guaranteed secure access (Bernard, 1996).

4. Encryption

Encryption is a technique of scrambling the characters in a message so they appear to be like random noise, with no discernible pattern. Only the recipient, who has the key, can unscramble the message.

5. TCP Wrapper

The TCP Wrapper is common solution that provides a good way of building an audit trail. It can filter incoming requests and log them based on the IP address and the service requested. It can also provide some protection against host name spoofing by verifying DNS name resolutions against more than one server. This is essentially asking for a second opinion about the authenticity of the remote host. (Bernard, 1996).

6. Network Security Scans

Use security scans to probe the network for weaknesses, before the hackers do.

Security scans indicate about 12% of hosts are vulnerable without a firewall and about 4% are vulnerable with a firewall. Firewalls give a false sense of security and can drastically degrade performance. However, the worst problem is PCs sharing drives. Also, many X Windows machines were found wide open - recommendation: shut off X Windows at the firewall. (Broersma, R., "The Network Security Threat", *San Diego Regional Info Watch Second Annual Network Security Symposium (SDRIW 97)*, San Diego, CA, 1997)

7. Email Filtering

Reject all email without either a sender or receiver in the organization's domain and log email activity. Do not allow the server to relay email! (Lawhorn, J., "The Network

Security Threat", *San Diego Regional Info Watch Second Annual Network Security Symposium (SDRIW 97)*, San Diego, CA, 1997)

8. Banners

Put a banner on the Web page warning that use of the site is subject to monitoring. This gives implied consent, which makes it easier to prosecute. If a user goes through the banner, then they cannot plead that they did not know.(McGuire, K., "Recent Prosecutions", *San Diego Regional Info Watch Second Annual Network Security Symposium (SDRIW 97)*, San Diego, CA, 1997)

9. Windows NT Security

There are 36 Windows NT exploits today. Microsoft provides service packs and hot fixes for known vulnerabilities, but it is up to you to properly configure the network. The default installation is not secure (permissions must be modified). Windows NT 4.0 has capabilities for access control, user account management, audits, packet filtering, and Remote Access Service (RAS) encryption. RAS is used to remotely log into a network. Some of the software tools available today are:

- Network scanners (ISS, KSA, NAT)
- Virus scanners (NAV, NTAV, McAfee)
- File and application encryption (PC Crypto, PC Secure, POTP Series)

- Network packet encryption (Centri TNT, NetCrypto)

(Brown, C., "Securing Your Windows NT Network from the Internet", *San Diego Regional Info Watch Second Annual Network Security Symposium (SDRIW 97)*, San Diego, CA, 1997)

Other recommendations for Windows NT security include:

- Use the Secure Sockets Layer (SSL) for encryption
- Enforce good passwords for user accounts
- Eliminate the Everyone group (anonymous users)
- Disable browser directory access (hide the directory structure)
- Disable LAN service (NETBIOS) for the Internet

(Duncan, R., "Security Considerations for NT Web Servers", *San Diego Regional Info Watch Second Annual Network Security Symposium (SDRIW 97)*, San Diego, CA, 1997)

10. UNIX Security

Security recommendations for UNIX include:

- Systems Access -- control who can log on or run programs (the most important way to protect the system)
- Accounts -- use auto-expiring accounts, inactivate unused accounts, and force password changes
- Password management -- See FIPS-181 (easily remembered passwords)
- UNIX -- tightly restrict root access and define functions by level
- System Auditing -- record login successes and login failures (especially watch for the Substitute User (SU) command)

(Walsall, P., "Multi-level Security for Open Systems", *San Diego Regional Info Watch Second Annual Network Security Symposium (SDRIW 97)*, San Diego, CA, 1997)

11. Email Privacy and Security

Different trust models are used. These include direct, hierarchical, and web of trust (e.g., Pretty Good Privacy (PGP) format). The most popular message formats are classic PGP, S/MIME, and PGP/MIME, but PGP cannot be used outside the US, because it uses strong algorithms. A new standard is Security Multi-part Encrypted, Multi-part Signed (RFC 1847). Remember that if a message can be broken, it will be broken. (Noerenberg, J., "Email Privacy and Security Issues", *San Diego Regional Info Watch Second Annual Network Security Symposium (SDRIW 97)*, San Diego, CA, 1997)

C. REFERENCES

This section lists some suggested references, covering various aspects of security.

1. Windows NT Security

Rutstein, C. B., *National Computer Security Association Guide To Windows NT Security*, McGraw-Hill 1997. This book has chapters on security architecture, managing user security, managing file and printer security, security logging and auditing, the Registry, designing secure NT networks, system integrity and availability, Remote-Access Service security, and NT Internet security. It has

appendices on Kerberos authentication, Passcrack, security-related event IDs, single sign-on security, and a pragmatic security checklist.

2. UNIX Security

Garfinkel, S. and Spafford, G., *Practical UNIX and Internet Security*, 1996. See this book for a comprehensive discussion of UNIX security.

3. Web Server Security

Bernard, R., *The Corporate Intranet: Create and Manage an Internal Web for Your Organization*, pp. 377-380 (Appendix D), Wiley Computer Publishing, 1996. One of the topics discussed in this book is Web server security. Appendix D explains, with examples, how to set up various configuration files. This enables the Web site administrator to restrict everything at a site, to limit access to a set of files, to authorize groups of users, or to limit access by machine location.

Another source of information is http://nmcs.com, which has advise on setting up a secure Web site (Milligan, N., "Setting Up a Secure Web Site", ", *San Diego Regional Info Watch Second Annual Network Security Symposium (SDRIW 97)*, San Diego, CA, 1997)

VII. CONCLUSIONS AND IMPLICATIONS

A. CONCLUSIONS

Several major issues were introduced and then discussed in the thesis.

The control issue, meaning who is in control, was shown to be a common theme in debates about centralized versus distributed computing, thin versus fat client, closed versus open access, supplier push versus user pull, and management control versus employee empowerment.

Another issue discussed is what role Web technology should play in an organization's IT strategy. One conclusion is that Web servers should be used for publishing documents and time-sensitive information and for interacting with users. Another is that Web Clients (browsers) should be used as a universal front end (user interface) to all back-end applications. Java will also play an important role because it allows data to be downloaded from a network with whatever programming is needed to display or playback the data (e.g., to playback a multimedia presentation). Finally, it was concluded that a bottom-up approach to intranet development is the preferred approach. This means that employees are encouraged to develop personal, workgroup, and functional Web sites, accessible inside the intranet, to share their corporate knowledge.

The issue of what kind of network architecture to use was also discussed. A good architecture uses a firewall to segment the network into three parts. The three parts are the Internet, the intranet, and the DMZ (or perimeter net). People in the extranet access the DMZ.

The issue of how to protect the intranet from network security threats, without excessively affecting productivity was discussed in terms of a number of common threats and countermeasures. While no network is 100% safe, a good strategy and vigilant efforts by knowledgeable experts can provide a reasonable tradeoff.

There is already more information written about intranets that can be read in a reasonable amount of time. For those who want to delve deeper into the subject, a number of references are provided, including the URLs for 94 intranet-related Web sites browsed during the literature search for this thesis.

B. RECOMMENDATIONS

An organization should provide a Web browser for each employee. An effective way to do this is to buy a site license and subscription for free upgrades. The software can be downloaded from an enterprise server. Web browsers are inexpensive, easy to use, and people like using them. This also lets corporate application developers focus on the back end, application development, knowing the front end

that will be used to interact with it (the current, site licensed, Web browser).

An organization should also provide Web server software for each employee and encourage its use on the intranet. This is probably the best way to quickly get corporate knowledge on-line so it can be shared, and reap the resulting benefits.

Management should hold employees accountable for their Web sites and their Web browsing. Information on Web sites should be restricted to the intranet, until it can be formally reviewed and approved for public release. This is to prevent the inadvertent or intentional release of sensitive information that could cause damage to the organization. Acceptable use policies and packet filtering in the firewall can improve the chances that Web browsing privileges are not used inappropriately.

Management should make network security a high priority. The openness that has made information so easy to access has also made it easy to compromise sensitive information. In addition, there are thousands of people on the Internet who have made it their objective to try to break into computer networks either for the challenge, for revenge, or for profit. The threat is too great to be ignored.

APPENDIX A. SAMPLE HTML FOR THESIS COVER PAGE

```
<HTML>
<HEAD>
   <META HTTP-EQUIV="Content-Type" CONTENT="text/html;
charset=iso-8859-1">
   <META NAME="Generator" CONTENT="Microsoft Word 97">
   <META NAME="Template"
CONTENT="E:\MSOFFICE\WINWORD\nps_thes.dot">
   <META NAME="GENERATOR" CONTENT="Mozilla/4.01 [en] (WinNT;
I) [Netscape]">
   <TITLE>COVER</TITLE>
</HEAD>
<BODY>

<CENTER>
<HR WIDTH="100%"></CENTER>

<CENTER><B><FONT SIZE=+3>NAVAL POSTGRADUATE
SCHOOL</FONT></B></CENTER>

<CENTER><B><FONT SIZE=+3>Monterey,
California</FONT></B></CENTER>

<CENTER> </CENTER>

<CENTER><IMG SRC="Image4.gif" VSPACE=96 HEIGHT=166
WIDTH=166></CENTER>

<CENTER><B><FONT SIZE=+3>THESIS</FONT></B></CENTER>

<CENTER> </CENTER>

<CENTER><TABLE BORDER CELLSPACING=3 CELLPADDING=7
WIDTH="432" >
<TR ALIGN=CENTER>
<TD VALIGN=TOP COLSPAN="2" HEIGHT="140">
<CENTER><B><FONT FACE="Times New Roman,Times">A PRACTICAL
GUIDE TO INTRANET
PLANNING</FONT></B></CENTER>

<CENTER><BR>
<FONT FACE="Times New Roman,Times">by</FONT></CENTER>

<CENTER><BR>
<FONT FACE="Times New Roman,Times">Charles D.
Kleinhans</FONT></CENTER>
```

```
<CENTER><BR>
<FONT FACE="Times New Roman,Times">September
1997</FONT></CENTER>

<CENTER> </CENTER>

<CENTER> </CENTER>

<CENTER> </CENTER>

<CENTER><FONT FACE="Times New Roman,Times">Thesis
Advisor:        &nbs
p;         &nbs
p;         &nbs
p;         &nbs
p;         &nbs
p;       
G. M. Lundy </FONT></CENTER> .

<CENTER> </CENTER>
</TD>
</TR>
</TABLE></CENTER>

<CENTER><B><FONT SIZE=-1> </FONT></B></CENTER>

<CENTER><B>Approved for public release; distribution is
unlimited.</B></CENTER>
```

APPENDIX B. INTRANET-RELATED WEB SITES

Intranet-related Web sites, discovered while doing research for this thesis, are listed below. The list was compiled as follows: First, each of the Internet search engines listed in Appendix C was used to search for the word *intranet*. Next, the first 20 hits found by each search engine were browsed until a decision could be made regarding the value of the information at the site. Finally, those sites judged to be potentially useful in the preparation of this thesis were saved as Web browser bookmarks. The title and Uniform Resource Locator (URL) for each Web site are shown.

Advertorial (Home for Intranet Planners),
http://www.interactivate.com/public/hip/hip-ads.html

Advise Paper: IBM's Intranet Offerings: Pathways to New Heights,
http://www.csc.ibm.com/advisor/library/2e76_135a.html

Allaire Corp., http://www.allaire.com/

AltaVista Search: Simple Query intranet,
http://altavista.digital.com/cgi-bin/query?pg=q&what=web&fmt=.&q=intranet

An Internet Intranet Co. Web Design Group Chicago,
http://www.wwwebdesign.com/

Articles On Intranet,
http://www.intrack.com/intranet/articles.shtml

Basic Facts, http://www.cam.org/~inagaki/webartic.html

Browser/Server(TM) Computing, http://browser-server.com/3.html

Building a Corporate Intranet - Welcome Page, http://webcom.com/wordmark/sem_1.html

Catalyst Intrnet Systems Intranet Information Site, http://www.catequity.com/

Chamomile, http://www.chamomile.demon.co.uk/index.html

Claremont Intranet Study - Table of Contents, http://www.clrmnt.com/sgi/toc.html#contents

Client-Server: Can It Be Saved?, http://techweb.cmp.com/iw/574/74mttra.htm

CNET - NEWS.COM - Intranets, http://news.com/Categories/Index/0,3,3,00.html?ntb.intrnt

Commerce At Light Speed, http://www.cals.com/

Customer Connection, http://www.bbn.com/customer_connection/

CW Net Central, http://pubsys.cmp.com/cw/cwi/netcentral/resource.html

Cybrargonians on the Net #6, http://www.teleport.com/~tbchad/cybrar/cybrar6.html

DataViews Homepage, http://www.dvcorp.com/

David Strom's Web Informant, http://www.strom.com/

Deja News - The Source for Internet Newsgroups!,
http://www.dejanews.com/

Finding the Right Intranet Technologies to buy,
http://www.strom.com/pubwork/intra2.html

FISH INTERACTIVE: STRATEGY FOR MEDIUM AND LARGE BUSINESSES,
http://www.fishmarket.com/1biz.html

http://www.jyu.fi/~maihama/linkit.html,
http://www.jyu.fi/~maihama/linkit.html

I2BS Intnet/Intranet Business Solutions, LLC.,
http://www.i2bs.com/

Infoseek, http://software.infoseek.com/map.htm

Infoseek: Whitepapers,
http://www.infoseek.com/Intranet_whitepapers?sv=N3&lk=noframes

Infoweavers Services,
http://www.infoweavers.com/text/services.html#anchor495445

Inktomi Corporation, http://www.inktomi.com/

InMagic, http://www.inmagic.com/

IntraNeT,
http://www.ilr.interbusiness.it/News/E_IntraNeT.htm

INTRANET, http://marvin.macc.wisc.edu/

Intranet 2001, http://www.inet2001.com/

Intranet Advisor - Intranet Education, Q & A, and Integration, http://ds.internic.net/cgi-bin/enthtml/business/intranet-advisor.b

Intranet and Internet Publishing,
http://www.nim.com.au/inet_pub/inet_pub.htm

Intranet Australia - Intranet Resources,
http://www.intra.net.au/noframes/vendor.htm

Intranet Communications Corporation,
http://www.intranetcommunications.com/

Intranet Construction Site, http://techweb.cmp.com/intranet-build/default.htm

Intranet Design: Emerging Standards Series,
http://www.innergy.com/foundation.html

Intranet Design: Home, http://www.innergy.com/

Intranet Exchange: The Web Professional's Forum,
http://www.innergy.com/ix/

INTRANET FAQs, http://www.intrack.com/intranet/ifaq.shtml

Intranet Information Page,
http://webcompare.iworld.com/intranet.html

Intranet Introduction,
http://www.intrack.com/intranet/introd.shtml

Intranet Library, http://www.rhinrichs.com/library.htm

IntraNet Links, http://www.abo.fi/~sasp/intra.htm

Intranet Paper, http://www.strom.com/pubwork/intranetp.html

Intranet Resources,
http://www.strom.com/pubwork/intranet.html

Intranet search engines rev up 10/7/96,
http://www.computerworld.com/search/AT-html/9610/961007SL1007sea3.html

Intranet Solutions,
http://home.netscape.com/comprod/at_work/index.html

Intranet White Paper,
http://www.process.com/intranets/wp2.htp

Intranet Whitepaper,
http://www.intrack.com/intranet/wpapers.shtml

Intranets deliver Internet technology ...,
http://www.inquiry.com/publication/infoworld/1996/issue08/INFO19960219e01-08.61.html

Intranets Unleashed, http://www.intranetsu.com/

Intranets, Imaging, Document Management, Workflow, & BPR,
http://www.infotivity.com/intrahom.htm

Intranets: What? Why? How?: @BRINT (tm),
http://www.brint.com/Intranets.htm

Links to Information about Intranets,
http://www.aloha.net/~dusty/intranets.html

Lycos search: intranet, http://www.lycos.com/cgi-bin/pursuit?query=intranet&searchButton.x=42&searchButton.y=13

McQueen Consulting, http://www.mcq.com/

Microsoft Announces Availability Of Personal Web Server For Windows, http://www.cam.org/home/Wcoprod/mmcomm/131.htm

Millennium Cybernetics, http://www.interactive.com/

MKS, Mortice Kern Systems, Inc., http://www.mks.com/

Money Daily: Info "pushers" proliferate on the Web, http://pathfinder.com/@@JKXvCQcAo7J7mX*1/money/moneydaily/1996/961008.moneyonline.html

MonoGraphics offers Intranet and Internet Site Design and Management, http://www.monographics.com/

Net Page,Inc. Custom Website Design, http://www.netpage1.com/

NetScape World, http://www.netscapeworld.com/

NetScheme, http://www.netscheme.com/

Network Computing, http://techweb.cmp.com:80/nc/netdesign/series.htm

NeuroSystems, http://www.neurosystems.com/

Open Market Intranet and Enterprise Products, http://www.openmarket.com/segments/intranet/

Open Market Intrnet and Enterprise Products, http://website-1.openmarket.com/segments/intranet/

Open Text Livelink Intranet, http://www.opentext.com/

PC Magazine: An Intranet Glossary, http://www.pcmag.com/issues/1508/pcmg0044.htm

resources - info source - glossary - Intranet, http://www.cnet.com/Resources/Info/Glossary/Terms/intranet.html

SEARCH'97 Information Server - Default Template, http://www.albert2.com/vtopic.vts

Selected MetaCrawler Search Results: Intranet, http://www.oac.uci.edu/indiv/franklin/Talks/960224/intranetrefs.html

Stardust Technologies, Inc., http://www.stardust.com/

Strategies from an intranet evangelist, http://www.computerworld.com/search/AT-html/9608/960819SL34book.html

The Complete intranet Resource, http://www.intrack.com/intranet/

The Intranet, http://www.hummingbird.com/whites/intranet.html

The Intranet Journal, http://www.intranetjournal.com/

The Resources of CIO Communications, Inc., http://www.cio.com/

The WDVL: Books, http://www.stars.com/Vlib/Reference/Books.html

The WDVL: Catalogs, http://www.stars.com/Vlib/Reference/Catalogs.html

The WDVL: Virtual_Libraries, http://www.stars.com/Vlib/Reference/Virtual_Libraries.html

Timefields Intranet Development, http://www.time-fld.demon.co.uk/inetdev.html

TradeWave Corporation,
http://galaxy.einet.net/tradewave/tradewave.html

Tympani Development, http://www.tympani.com/

US Web, http://www.usweb.com/pressroom/buzz/970415_cnet.html

Welcome to Intrnut, http://www.intranut.com//index.htm

Wordmark.Com Home Page, http://wordmark.com/

Yahoo! - Computers and Internet:Communications and Networking:Intr,
http://www.yahoo.com/Computers_and_Internet/Communications_and_Networking/Intranet/Intranet_Design_Magazine/

Yahoo! - Computers_and_Internet/Communications_and_Networking/Intranet/,
http://www.yahoo.com/Computers_and_Internet/Communications_and_Networking/Intranet/

Yahoo! Search Results,
http://search.yahoo.com/bin/search?p=intranet

APPENDIX C. INTERNET SEARCH ENGINES

The Internet search engines listed below were used to find the intranet-related Web sites listed in Appendix B.

100hot Websites, http://www.100hot.com/

A Business Compass Home Page, http://www.abcompass.com/

Albert 2 Table of Contents, http://www.albert2.com/

AltaVista Technology, Inc., http://www.altavista.com/

CyberHound, http://www.cyberhound.com/

DOWNLOAD.COM - Welcome,
http://www.download.com/?netscape.dlbtn

Excite Home, http://www.excite.com/

go2net | MetaCrawler, http://www.metacrawler.com/

HotBot,
http://www.hotbot.com/IU0JNEXRAD4E629912213839EE46F9D75075BA49/index.html

Infoseek, http://www.infoseek.com/Home?pg=Home.html&sv=N3

LinkStar, http://www.linkstar.com/linkstar/bin/dosearch-linkstar

LookSmart - exploring LookSmart,
http://mulwala.looksmart.com:8080/?comefrom=netscape&divert

Reference.COM Search, http://www.reference.com/

Search the Galaxy, http://www.einet.net/cgi-bin/wais-text-multi?

The Argus Clearinghouse, http://www.clearinghouse.net/

The Open Text Index, http://index.opentext.net/

WebCrawler Searching, http://webcrawler.com/

Welcome to Lycos, http://www.lycos.com/

Welcome to Magellan!, http://www.mckinley.com/

Welcome to the Electric Library, http://www3.elibrary.com/id/2525/search.cgi

Yahoo!, http://www.yahoo.com/

LIST OF REFERENCES

Bernard, R., *The Corporate Intranet: Create and Manage an Internal Web for Your Organization*, pp. 3, 12-13, 23, 64, 279, 306-307, 310, 315-316, 324, 377-380, Wiley Computer Publishing, 1996.

Broersma, R., "The Network Security Threat", *San Diego Regional Info Watch Second Annual Network Security Symposium (SDRIW 97)*, San Diego, CA, 1997.

Brown, C., "Securing Your Windows NT Network from the Internet", *San Diego Regional Info Watch Second Annual Network Security Symposium (SDRIW 97)*, San Diego, CA, 1997.

Carroll, M. L., *Cyberstrategies, How To Build an Internet-Based Information System*, pp. 2-3, 21, 150, 153, 265, Van Nostrand Reinhold, 1996.

Developing With Java, pp. 3-8, Paradigm Research, Inc., 1997.

Duncan, R., "Security Considerations for NT Web Servers", *San Diego Regional Info Watch Second Annual Network Security Symposium (SDRIW 97)*, San Diego, CA, 1997.

Federal Standard 1037C: Glossary of Telecommunication Terms, http://www.its.bldrdoc.gov/fs-1037/

Garfinkel, S. and Spafford, G., *Practical UNIX and Internet Security*, 1996.

Gibbs, M. and Smith, R. J., *Navigating the Internet*, pp. 24, Sams Publishing, 1993.

Haack, P., "Firewalls and Proxy Services", *San Diego Regional Info Watch Second Annual Network Security Symposium (SDRIW 97)*, San Diego, CA, 1997.

Karn, P, "Security Issues in Wireless Communications", *San Diego Regional Info Watch Second Annual Network Security Symposium (SDRIW 97)*, San Diego, CA, 1997.

Lawhorn, J., "The Network Security Threat", *San Diego Regional Info Watch Second Annual Network Security Symposium (SDRIW 97)*, San Diego, CA, 1997.

McGuire, K, *San Diego Regional Info Watch Second Annual Network Security Symposium (SDRIW 97)*, San Diego, CA, 1997.

Milligan, N., "Setting Up a Secure Web Site", ", *San Diego Regional Info Watch Second Annual Network Security Symposium (SDRIW 97)*, San Diego, CA, 1997.

Nangle, K., "Firewalls Guard the Network DMZ", pp. 135-138, *ZD Internet Magazine*, June 1997.

National Software Testing Laboratories, Inc., "About to buy a firewall? Read this first", pp. 35-40, *Government Computer News*, August 4, 1997.

Noerenberg, J., "Email Privacy and Security Issues", *San Diego Regional Info Watch Second Annual Network Security Symposium (SDRIW 97)*, San Diego, CA, 1997.

Perrine, T., "The Network Security Threat", *San Diego Regional Info Watch Second Annual Network Security Symposium (SDRIW 97)*, San Diego, CA, 1997.

Rutstein, C. B., *National Computer Security Association Guide Tto Windows NT Security*, pp. 321-327, McGraw-Hill 1997.

Tanenbaum, A. S., *Computer Networks*, pp. 3-4, 11-12, 17, 37, 301, 410-412, Prentice Hall, Inc., 1996.

TechWeb Technology Encyclopedia,

http://www.techweb.com/encyclopedia/defineterm.cgi

Walsall, P., "Multi-level Security for Open Systems", *San Diego Regional Info Watch Second Annual Network Security Symposium (SDRIW 97)*, San Diego, CA, 1997.

"Who needs a Network Computer?", pp.96, *Datamation*, Oct 1996.

BIBLIOGRAPHY

"Bridge your legacy systems to the Web", pp.119, *Datamation*, Mar 97.

Brutzman, D. P., Macedonia, M. R. and Zyda, M. J., Internetwork *Infrastructure Requirements for Virtual Environments*. Proceedings of the NII 2000 Forum of the Computer Science and Telecommunications Board, National Research Council, Washington, DC, 23-24 May 1995. Also accepted for publication in the Proceedings of the 1995 Symposium on VRML.

Hsiao, D. K., *Strategies in the Microprocessor Industry to TCP/IP Interconnecting: Concepts, Architecture, Protocols, and Tools*, in Encyclopedia of Microcomputers (Editors: Kent, A., Williams, W., Hall, C. M. and Kent, R.), Marcel Dekker, Inc. 1995.

Irvine, C., *Report on the Defensive Information Warfare Symposium*, Electronic Cipher #3, Dec. 23, 1995, IEEE Computer Society TC on Security and Privacy. URL http://www.itd.nrl.navy.mil/ITD/5540/ieee/cipher/

Lewis, T., *Where is Client/Server Software Headed*: IEEE Computer, 28, no. 4, April 1995, pp. 49-55.

Macedonia, M. R., Zydam M. J., Pratt, D. R., Brutzman, D. P. and Barham, P. T., *Building Large-Scale Virtual Environments: A Network Software Architecture*. Proceedings of Industrial Virtual Reality 1995, Tokyo, Japan (as invited speaker), 28-30 June 1995, pp. 18-28.

"Middleware: Link everything to anything", pp. 119, *Datamation*, Oct 96.

GLOSSARY

Technical terms used in this thesis are defined in the glossary. For more detailed definitions or for definitions not included here, the following sources are suggested:

(1) Federal Standard 1037C: Glossary of Telecommunication Terms, http://www.its.bldrdoc.gov/fs-1037/

(2) TechWeb Technology Encyclopedia, http://www.techweb.com/encyclopedia/defineterm.cgi

Anonymous user - A person who logs in to a computer without using a user ID and password supplied by the system administrator (there is no individual user account). Typically, the user enters *anonymous* for the user ID and their email address for the password, when prompted.

Applet - A Java program that is downloaded from a Web server and run in the Web browser when a Web page containing a reference to the applet is accessed. Note that a Java applet is different than a Java application (see Table 3 for a comparison).

Application (level) gateway - See gateway.

Application - A computer program that a user runs.

Assembly languages (second generation languages) - A low level computer programming language that uses alphanumeric symbols for instructions, as opposed to machine

language programs, which use only ones and zeros for instructions.

Backbone - The main, high speed, high capacity, circuit in a network that carries data from many lower speed, lower capacity circuits.

Batch job - A program that is run as a unit from beginning to end, as opposed to an interactive program. Derives from when computer programs were keypunched into a deck of cards. The program decks from many different programs were put together and run as a "batch job", usually overnight, with the results available the next day.

Bridge - A device that connects two or more *similar* networks.

Broadcast - A type of network where a single medium is shared by a number of devices (e.g., Ethernet™). When one computer transmits all hear the transmission. If more than one transmits at the same time there is a collision, then both wait a random amount of time and try again.

Cached - Stored in memory for fast access.

Central Processing Unit (CPU) - The part of a computer that executes instructions and does numerical computations. Essentially the brain of the computer system.

Centralized computing versus distributed computing - Centralize computing shares a single computer among many users (e.g., a single mainframe). Distributed computing

distributes the computing power among many different computers (e.g., many PCs in a network).

Client - See Client-Server.

Client-Server - For hardware, when a central computer (server) shares information with local workstations (clients). For software, when an application is split into two parts. The part that runs on the user's workstation is the client software. The part that runs on the server is the server software.

Closed access versus open access - The default is no access with the closed access model. The default is full access with the open access model.

Common Gateway Interface (CGI) - A standard application programming interface that allows Web servers to communicate with back end processes like databases. The program is a CGI script.

Compilation - The process of compiling (translating) a computer program written in source code (Ada, C, C++, etc.) into machine language for a particular target machine architecture (Mac, DOS PC, etc.).

Cracker - A person who breaks into a computer system or network with malicious intent.

Demilitarized Zone (DMZ) - Also called a perimeter network. A separate network segment that has limited public access through a firewall. Part of an organization's

network, but one with public access allowed. People in the organization's extranet would typically access servers in the DMZ. See figure 11 for a more detailed explanation.

Denial of service attack - A type of computer attack where the intent is to deny service to legitimate users by straining the capacity of the targeted system. As an example, someone could flood an email server with millions of mail messages. If the attack is severe enough, it could slow response to a crawl or cause buffers to overflow and cause the system to crash.

Dialup networking - A method of connecting to a remote computer network by dialing up a pre-arranged phone number and having a connection automatically made by the network. The user, who initiates the call, uses a modem to communicate through telephone lines. A Remote Access Service manages this kind of connection.

Diskless workstation (diskless thin client) - A PC with no hard drive or operating system (use microkernals instead). Applications run on the server. (Datamation, Oct 96)

Distributed Queue Dual Bus (DQDB) - IEEE 802.6 standard for Metropolitan Area Networks. See Figure 5.

Domain - The highest level of the hierarchical naming system used with IP addressing. For example, in the URL

http://www.companyname.com, com (which stands for commmercial) is the domain.

Domain Name System (DNS) - The naming system that is used to translate alphanumeric addresses into numeric addresses and vice versa.

Encryption - Encryption is a technique of scrambling the characters in a message so they appear to be like random noise, with no discernible pattern. Only the recipient, who has the key, can unscramble the message.

Ethernet™ - IEEE 802.3 standard for networking. It uses a bus topology, is a broadcast network, operating at 10 Mbps.

Extranet - The part of an organization's private network that is made accessible to suppliers, distributors, dealers, business partners, etc.

File Transfer Protocol (FTP) - The application level protocol that is part of the TCP/IP protocol suite that provides services for copying files across a network.

Firewall - A network device (hardware and software) the is put between an organization's private internal network and the Internet to prevent unauthorized public access to the private network.

Gateway - A device that connects two or more networks using different protocols.

Gigabyte (GB) - 2^{10} or 1024 Mb.

Hacker - A person who tries to break into computer systems or networks.

High order languages (third generation languages) - A high level procedural computer programming language (e.g., C, C++, Ada, Fortran, Cobol, Algol, PL1, Basic, etc.) that is much higher than assembly language. One high order language statement is equivalent to perhaps 5-10 assembly language statements. This makes it much faster to create a program than in assembly language.

HTML markup tags - Sequences of text characters enclosed in angle brackets that are interpreted by the Web browser for displaying a document written in HTML. For instance <H1>This is the highest level heading in HTML.</H1> displays the enclosed text using a font specified for H1 in the browser preferences.

Hub - A device that interconnects one or more workstations (typically) to a network backbone. See figure 11.

Hypertext links - Text that contains a link to another document. Clicking on a hypertext link causes the Web client to send a request for a document to the Web server specified in the link. The Web server sends the specified document back to the requesting client (Web browser). A browser typically shows links underlined and colored blue, although users can change these settings.

Hypertext Markup Language (HTML) - A standard way of marking up text with tags to specify how a document is to be displayed.

Hypertext Transfer Protocol (HTTP) - The protocol used for communication between Web clients and Web servers.

Independent Software Vendor (ISV) - Vendors who produce commercial off-the-shelf software products.

Institute of Electrical and Electronic Engineers (IEEE) - An organization which, among other things, produces widely accepted standards, such as the networking standards mentioned in this thesis.

Internet - The world wide internetwork that connects various WANs from around the world. The Internet uses the TCP/IP protocol suite for communication.

Internet Protocol (IP) - The network layer protocol in the TCP/IP protocol suite.

Internet search engines - A software tool used to search the Internet for a specified search string. The result is a list of the sites satisfying the search criteria.

Internet Service Provider (ISP) - A commercial vendor that supplies and connection to the Internet for a monthly fee.

Interpreter - A computer program that "interprets" source code. An interpreter differs from a compiler in that

an interpreter translates and then executes each statement of source code one statement at a time, while a compiler translates the entire source code program to an executable program before any of the resulting machine language program is executed.

Intranet (internal Web) - An organization's internal, private network (inside the firewall), that uses Internet technology, such as the TCP/IP protocol stack, Web servers and Web clients.

IP address (source and destination) - An IP address is the unique, world-wide network address of a host computer. It uniquely identifies a particular computer. An IP address is a 32 bit number represented as a series of four octal numbers separated by dots, such as 195.252.75.60. The IP address can be translated to a host name and domain name, such as myname@cs.nps.navy.mil using the Domain Naming Service. An IP packet contains both a source address (where the packet is coming from) and a destination address (where the packet is going to).

Java - An object-oriented programming language which has features especially designed for Web use. A Java program may be either an applet or an application. See table 3 for a comparison.

Just-in-time inventory system - An inventory system which seeks to minimize inventory levels and the cost of

inventory by delivering the supplies that are needed, just-in-time for their use in the manufacturing process.

Kerberos authentication - An authentication protocol. For a description, see Tanenbaum, 1996.

Local Area Networks (LAN) - A network that is limited in geographical area to a room, building, ship, or aircraft. LANs may be interconnected to form campus networks, MANs, or WANs.

Mail bomb - An example of a denial of service attack caused by repeatedly sending email to a valid user account and overwhelming system resources trying to process the incoming mail (Carroll, 1996).

Management control versus employee empowerment - The issue of how much control should management and the IT staff have versus how much control should employees, workgroups, and divsions have. See the discussion of this issue in Chapter III.

Megabyte (MB) - 2^{10} or 1024 Kb.

Metropolitan Area Network (MAN) - A network that covers a metropolitan area (city-wide).

Middleware - Software that sits between two incompatible pieces of software and makes the necessary translations to make them interoperate.

Modem - A device that is used to transmit digital data over an analog telephone circuit.

NetBIOS - A network protocol for PC LANs. NetBIOS and NetBEUI (an extended version of NetBIOS) are used on all Windows-based operating systems that support networking. They cannot be used for internetworking because the protocol cannot be routed.

Network architecture - A definition of the network structure, components, and arrangement of components.

Network PC (NC or NetPC) - A slimmed down version, of a PC, promoted by Microsoft, and designed specifically for business, is called a NetPC. It has less memory and is not customizable by users, which reduces administration costs. The version promoted by Oracle and Sun is called the Network Computer or NC. It is slimmed down even further, and the hard disk is optional, since all storage is expected to be on the network.

Packet - A collection of bits, treated as a unit, which are transmitted by a packet switching network. A packet contains fields for source and destination address, data, and control elements.

Packet-filtering router - A router, which examines each packet's source and destination address and either forwards or drops the packet, depending on the rules defined in router tables.

Perimeter net - See Demilitarized Zone (DMZ).

Personal Identification Number (PIN) - A secret code number that identifies the holder as an authorized user.

Point-to-Point Protocol (PPP) - A data link protocol that enables a computer to access the Internet over a telephone line with a modem. It is used to send IP packets over a serial line. PPP was developed by the Internet Engineering Task Force and has become very popular for Internet access.

Port number - Port numbers identify the type of service requested (e.g., Telnet, FTP, HTTP).

Pretty Good Privacy (PGP) - A public key cryptography method.

Protocol - A standard set of rules or conventions governing how communication will be done.

Proxy server - An intermediate server, between the requesting machine and the server the request is going to. The proxy server relays the request and the reply on behalf of the requesting machine.

Regional network - A network that covers a particular geographical region. It is larger than a LAN and smaller than a WAN.

Remote Access Service (RAS) - A service provided by Windows that enables users to remotely login to a computer through a modem.

Root access - On a UNIX system root access gives the user complete control of the computer.

Router - A network device that routes packets from one LAN or WAN to another.

San Diego Regional Info Watch (SDRIW) - An organization that acts as a regional Computer Emergency Response Team (CERT) and neighborhood watch for the San Diego area.

Screened subnet - See Demilitarized Zone (DMZ).

Search engines - See Internet search engines.

Secure Multipurpose Internet Mail Extensions (S/MIME) - MIME is a standard for transmitting non text files over Internet email. Secure MIME is an extension which uses RSA public key encryption for secure transmissions.

Secure Sockets Layer (SSL) - A protocol by Netscape for making secure transactions of the Web. SSL provides encryption and authentication.

Server - See Client-Server.

Simple Mail Transfer Protocol (SMTP) - An application layer, TCP/IP protocol that defines email message format for ASCII text. MIME extends SMTP to handle multimedia email attachments.

Serial Line Internet Protocol (SLIP) - A data link protocol that enables a computer to access the Internet over a telephone line with a modem. It is used to send IP packets over a serial line.

Sniffer - Hardware or software that monitors packets and is used to find bottlenecks in a network.

Snooping - By using a sniffer, a snooper see the unencrypted character stream typed by a user during a login, thus discovering the userid and password for a subsequent break-in.

SPAM - Unsolicited commercial email.

Spoofing - Spoofing is a technique of changing the address in the IP packet to fool the firewall into thinking the packet came from an address (inside the network) that will not be blocked. Spoofing IP addresses is very easy (Carroll, 1996).

Structured Query Language (SQL) - A standard language developed for querying relational databases.

Subnet - A collection of routers and transmission lines - no hosts.

Supplier push versus user pull - Supplier push refers to the originator of a message pushing the message to the intended recipients. Email, fax, and the telephone are examples of push technologies. User pull refers to the recipient retrieving a message (pull) whenever the user chooses to do so. The Web is considered a pull technology (although push technology will soon be added).

Syn flooding - A denial of service attack (also known as synchronize/start flooding or synchronize storms) where a

firewall is bombarded with requests to synchronize TCP connections. This causes the firewall to respond by allocating all available buffer space to these requests and denying legitimate connections. (National Software Testing Laboratories, Inc., 1997)

TCP sequence prediction - This is an attack that fools applications using IP addresses for authentication (e.g., UNIX rlogin and rsh commands) into thinking that bogus packets actually came from trusted machines. (National Software Testing Laboratories, Inc., 1997)

TCP wrapper - The TCP Wrapper is common solution that provides a good way of building an audit trail. It can filter incoming requests and log them based on the IP address and the service requested. It can also provide some protection against host name spoofing by verifying DNS name resolutions against more than one server. This is essentially asking for a second opinion about the authenticity of the remote host. (Bernard, 1996).

Telnet - A TCP/IP application layer service that provides the ability to login to a remote host.

Thin client versus fat client - A thin client is one where very little of the functionality resides in the client part of a client-server design. A fat client is where much functionality is present in the client.

Transmission Control Protocol (TCP) - A transport layer protocol in the TCP/IP protocol suite that provides connection-oriented host-to-host communications.

Transmission Control Protocol/Internet Protocol (TCP/IP) - A suite of inter-related protocols used to communicate over the Internet.

Uniform Resource Locator (URL) - The addressing scheme used by the World Wide Web. The format for a URL for a Web server is http://server_name/pathname/file.html.

US backbone - The main communications backbone in the United States.

User Datagram Protocol (UDP) - A transport layer protocol in the TCP/IP protocol suite that is used in place of TCP, if reliable delivery is not required, for instance, with real-time audio or video. In these cases, if a packet is missed it is simply ignored, because there is no time to retransmit it.

Virtual network - A group of interconnected networks that logically appear as a single network to the user.

Video Teleconferencing (VTC) - An interactive communications session where video and audio communications allow people who are geographically separated to meet electronically.

Wide Area Network (WAN) - A network that spans a large geographical area, such as a country or continent. It may link together LANs, MANs, and regional networks.

Web - See World Wide Web.

Web browser - A software program that runs on a desktop machine and acts as the client part of the client-server system. The two most popular Web browsers are Netscape Navigator and Microsoft Internet Explorer. Web browsers display Web pages written in HTML.

Web Site - See World Wide Web.

World Wide Web (WWW) - The world wide collection of Web servers and Web clients that implement the HTTP protocol for communication between client and server and the HTML protocol for displaying Web documents.

X Windows - A client-server windowing system developed at MIT. It is usually run on UNIX machines.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Rd., STE 0944
   Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Rd.
   Monterey, CA 93943-5101

3. Dr. Ted Lewis, Chairman 1
   Department of Computer Science, Code CS/L
   Naval Postgraduate School
   833 Dyer Rd.
   Monterey, CA 93943

4. Professor Bert Lundy 1
   Department of Computer Science, Code CS/LN
   Naval Postgraduate School
   833 Dyer Rd.
   Monterey, CA 93943

5. COMMANDING OFFICER 1
   ATTN DON SNIDER
   NCCOSC RDTE DIV D80
   53560 HULL ST
   SAN DIEGO CA 92152-5001

6. COMMANDING OFFICER 1
ATTN GALE PENNOYER
NCCOSC RDTE DIV D0204
53560 HULL ST
SAN DIEGO CA 92152-5001

7. COMMANDING OFFICER 1
ATTN DON MILSTEAD
NCCOSC RDTE DIV D80
53560 HULL ST
SAN DIEGO CA 92152-5001

8. COMMANDING OFFICER 1
ATTN BOB KOCHANSKI
NCCOSC RDTE DIV D82
53560 HULL ST
SAN DIEGO CA 92152-5001

9. COMMANDING OFFICER 1
ATTN FLOYD ROBINSON
NCCOSC RDTE DIV D828
53560 HULL ST
SAN DIEGO CA 92152-5001

10. COMMANDING OFFICER 2
ATTN CHARLES KLEINHANS
NCCOSC RDTE DIV D828
53560 HULL ST
SAN DIEGO CA 92152-5001

DUDLEY KNOX LIBRARY
NAVAL POSTGRADUATE SCHOOL
MONTEREY CA 93943-5101

DUDLEY KNOX LIBRARY
3 2768 00340859 2